Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Bezpečnost v Lotus Notes

Jakub Richtr

Česká zemědělská univerzita v Praze | Provozně ekonomická fakulta

Katedra informačních technologií | Akademický rok 2009/2010

ZADÁNÍ DIPLOMOVÉ PRÁCE

Jakub Richtr

obor Informatika

Vedoucí katedry Vám ve smyslu Studijního a zkušebního řádu ČZU v Praze čl. 17 odst. 2 určuje tuto diplomovou práci.

Název práce: **Bezpečnost v Lotus Notes**

Osnova diplomové práce:

1. Úvod
2. Cíl práce a metodika
3. Lotus Notes
4. Lotus Notes přes internet a mobilní telefon
5. Bezpečnost Lotus Notes
6. Závěr
7. Seznam použitých zdrojů
8. Přílohy

Rozsah hlavní textové části: 60 - 80 stran

Doporučené zdroje:

DAHM, F. a kol. Security Considerations in Lotus Notes and Domino 7, IBM Redbooks, 2006. ISBN 0738497347
LANDON a kol. iNotes Web Access on the IBM iSeries Server IBM Redbooks, 2002. ISBN 0738425206
MORAVEC, L.: Lotus Notes 7 uživatelská příručka, Grada, 2008, 255 str., ISBN 978-80-247-2346-4
TWOREK, W. a kol. Lotus Security Handbook, IBM Redbooks, 2004. ISBN 0738498467

Vedoucí diplomové práce: **Ing. Čestmír Halbich, CSc.**

Termín odevzdání diplomové práce: duben 2011

....

Vedoucí katedry Děkan

V Praze dne: 15. 1. 2010

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Bezpečnost v Lotus Notes" jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 4.4.2011 _____

Poděkování

Rád bych touto cestou poděkoval panu Ing. Čestmíru Halbichovi, CSc. Za jeho odborné vedení, podporu a věcné připomínky, které mi poskytl k vypracování této práce.

Bezpečnost v Lotus Notes

Security in Lotus Notes

Souhrn

Tato diplomová práce se zabývá bezpečností e-mailového klienta Lotus Notes. Analyzuje pojmy a principy, na kterých je postavena bezpečnost tohoto klienta a popisuje základní vlastnosti a charakteristiky, kterými se tento poštovní klient vyznačuje. V teoretické části jsou popsány způsoby užití klienta a způsoby možného nastavení jeho zabezpečení. Praktická část se následně zabývá implementací vhodného řešení dle požadovaného zadání. V praktické části je dále provedeno porovnání Lotus Notes s jeho alternativami. V závěru práce je proveden souhrn výsledků vlastní práce a je provedeno celkové zhodnocení.

Summary

This master thesis is aimed at research concerning security of Lotus Notes e-mail client. It analyzes procedures and fundamentals that are ground for security of this client and describes basic properties and characteristics that define the client. Theoretical part of the thesis contains various options and security settings of client. Practical part of the thesis aims at implementation of proper solution according to specific request. It also compares Lotus Notes client to other software possibilities. Conclusion of the thesis holds summary of results from the practical part and overall evaluation.

Klíčová slova: Poštovní databáze, Seznam přístupových práv, Databáze, Bezpečnost, Šifrování, skupiny, Webové rozhraní, Replikace, Certifikát, Podpis, Pracoviště

Keywords: Mailbox, Access Control List, Database, Security, Encryption, Groups, Web Interface, Replication, Certificate, Signature, Location

Obsah:

Obsah: 2
1 Úvod 3
2 Cíl práce a metodika 4
3 Lotus Notes 5
3.1 Verze Lotus Notes/Domino 5
3.2 Mobilní použití a replikace 12
3.3 Bezpečnost systému 14
3.3.1 Autentizace 14
3.3.2 Autorizace 16
3.3.3 Protokoly 26
3.3.4 Standardy 26
3.3.5 Specifické bezpečnostní požadavky 27
3.3.6 Přístup k serverům a certifikáty 27
3.3.7 ID Vault 30
4 Lotus Notes přes internet a mobilní telefon 31
4.1 LN přes internet 31
4.2 LN přes mobilní telefon 32
4.2.1 OneBridge 32
4.2.2 BlackBerry 34
4.2.3 Lotus Notes Traveler 35
5 Bezpečnost Lotus Notes 37
5.1 Zadání 37
5.2 Návrh řešení 37
5.2.1 Tvorba a nastavení uživatelského účtu 37
5.2.2 Delegování práv 46
5.2.3 Nastavení archivace 47
5.2.4 Tvorba skupin 49
5.2.5 Blokování uživatele 50
5.2.6 Tvorba a nastavení zástupné schránky 51
5.2.7 Lotus Traveler instalace a nastavení 53
5.2.6 Webové rozhraní 59
5.3 Shrnutí 60
5.3.1 Navržené řešení 60
5.3.2 Zjištěné nedostatky 61
5.4 Porovnání Lotus Notes s alternativami 61
6 Závěr 64
7 Seznam použitých zdrojů 66

1 Úvod

Poštovní klient je počítačový program, který slouží k přijímání či odesílání elektronické pošty. Klient nejčastěji stahuje poštu přes protokol POP3 na lokální disk a tím k ní umožňuje uživateli přístup. Další možností je vzdálený přístup k poště skrze IMAP. Pošta se nejčastěji odesílá protokolem SMTP. Poštovní klient umožňuje uživateli spravovat poštovní zprávy, kontakty, kalendář, úkoly, filtrovat nevyžádanou poštu či pracovat s diskusními skupinami. Mail user agent je počítačový program pro řízení e-mailů. Rozsáhlí poštovní klienti jako je Lotus Notes, Mozzila Thunderbird a Microsoft Outlook kombinují operace agentů Mail submission agent, Mail delivery agent, Mail retrieval agent a Mail user agent v jedné aplikaci. Mail user agent není sám schopen posílat a přijímat poštu. Jeho funkce spočívá v připojování k poštovní schránce, do které je e-mail přenesen a uložen v příslušném formátu. Mail user agent pak umožňuje základnímu uživatelskému rozhraní pracovat s poštou.

Hlavním bezpečnostním prvkem v e-mailové komunikaci je šifrování. Bez šifrování je e-mailová aktivita viditelná a kdokoli s přístupem k síti může sledovat e-maily a získat přihlašovací hesla. Šifrování e-mailů umožňuje zvýšit bezpečnost e-mailové komunikace a vyvarovat se těchto hrozeb. Užívají se dva typy šifrování. Prvním je šifrování relací, kdy všechny e-mailové protokoly mohou šifrovat celou relaci, aby nedošlo k odposlechu uživatelského jména a hesla. Druhým typem je šifrování těla zprávy. Pro něj se používají dva modely S/MIME a OpenPGP. Model S/MIME je založený na certifikační autoritě, která podepisuje uživatelské veřejné klíče. OpenPGP používá flexibilnější síť, která umožňuje uživatelům podepisovat jeden druhému veřejné klíče. V obou modelech je zašifrováno pouze tělo zprávy. Hlavičky, příjemci a předmět zůstávají ve formátu prostého textu.

Kromě poštovních klientů a malých Mail user agentů existují také poštovní programy nazývané webmail. Jejich hlavní výhodou je schopnost posílat a přijímat zprávy odkudkoliv pomocí aplikace internetového prohlížeče. To eliminuje potřebu nastavení MTA/ MRA/ MDA/ MUA řetězce. Mezi významné webmail klienty patří Hotmail, Gmail a Yahoo. Z českých je to například Seznam.cz, nebo Centrum.cz. [6]

2 Cíl práce a metodika

Cílem práce je zhodnotit bezpečnost e-mailového klienta Lotus Notes. A to z hlediska přístupu přes webové rozhraní, mobilní telefon a samotného klienta. I s následným navržením řešení dle požadovaného zadání, včetně ukázky nastavení klienta a porovnání bezpečnosti Lotus Notes s ostatními alternativami.

Metodika zpracování se dá rozdělit do několika základních částí. První část se zabývá shromažďováním potřebných podkladů o problematice bezpečnosti a možnostech využití poštovních klientů, zejména Lotus Notes. Informace jsou čerpány z odborné literatury a z internetu. Převážně z publikací IBM Redbooks a odborných portálů věnujících se problematice Lotus Notes. Další částí je příprava poznámek pro psaní vlastní práce na základě získaných informací. Neméně důležité je stažení, instalace a následné seznámení s trial verzí nejaktuálnější verze klienta Lotus Notes verze 8.5.2 z portálu IBM. Pro vlastní práci je vytvořen seznam požadavků fiktivního zadavatele. Tyto požadavky jsou následně vyhodnoceny a aplikovány na klienta Lotus Notes, který je dle požadavků nastaven. Tímto jsou demonstrovány možnosti tohoto klienta. Důraz je kladen na možnosti nastavení zabezpečení z pohledu klienta Lotus Notes. V závěru je proveden souhrn a zhodnocení praktické části.

Po dopsání hrubé práce je formálně upraven text včetně doplnění citací. Následně se provede revize obsahu, kontrola gramatiky a konečná formální úprava celé práce.

3 Lotus Notes

3.1 Verze Lotus Notes/Domino

Verze 1.0

Tato první verze aplikace Lotus Notes, byla nasazena na trh v roce 1989. Aplikace Lotus Notes obsahovala 536 484 řádků programového kódu a za první rok se prodalo 35 000 licencí. Její uživatelé mohli vytvářet, ale hlavně sdílet informace a data pomocí osobního počítače a lokální počítačové sítě. První verze nabízela grafické rozhraní, ve kterém bylo možné pracovat nejen pomocí klávesnice, ale i pomocí myši. Tato první verze byla vybudována na architektuře „*klient/server*“ a jejím hlavním znakem byly osobní počítače připojené do LAN. Lotus Notes klient bylo možné provozovat na operačním systému DOS 3.1 nebo OS/2 a Lotus Notes server vyžadoval operační systém DOS 3.1 nebo OS/2. Servery Lotus Notes si mezi sebou vyměňovaly informace a data pomocí replikace. Replikace umožňovala Lotus Notes distribuci dat na různá geografická místa a jejich nepřetržitou synchronizaci v libovolně nastavených periodách. První verze obsahovala k okamžitému použití aplikace Group Mail pro skupinovou elektronickou poštu, Group Discussion pro skupinovou diskuzi a Group Phone Book, neboli skupinový adresář. Do programu byla zahrnuta vlastnost aplikační flexibility, která umožňovala vytvořit si aplikace podle vlastní potřeby. V produktu byly obsaženy i šablony aplikací, které mohly napomoci při tvorbě vlastních aplikací a databází. Funkce, které nabízela tato verze byly například šifrování dat, elektronický podpis, nebo elektronické ověření pravosti s využitím public key technologie RSA. Lotus Notes se tak stal prvním významným komerčním systémem, který využíval technologii RSA. Mezi nejdůležitější rysy programu patřila již od počátku vysoká bezpečnost. K tomu přispělo zejména zavedení systému Access Control List (ACL). ACL je systém přístupových práv k databázím, který říká, kdo může přistoupit k jaké databázi a co v ní může dělat. Mezi další funkce patřila například možnost využití dial-up spojení mezi Notes servery a Notes klienty. Tato vlastnost umožňovala přenos informací a dat mimo prostředí LAN a podporovala tak uživatele Lotus Notes klienta, kteří do klienta přistupovali vzdáleně. Tato verze také umožňovala import a export informací a snadné odesílání a přijímání elektronických poštovních zpráv s možností nastavení automatického potvrzení o doručení zprávy. Verze 1.0 nabízela vytvoření

objektu typu DocLink, který umožňoval propojení dokumentů. Obsahovala také jednoduchý skriptovací programovací jazyk „*@Formula language*“, sloužící pro vytváření vlastních Notes aplikací a nástroj pro administraci serverů a klientů Notes. Většina těchto vlastností a funkcí patřila v roce 1989 mezi revoluční novinky. [3, s. 20]

Verze 1.1

Verze 1.1 přinesla první vylepšení. Na trh přišla v roce 1990 a neobsahovala žádné zvláštní nové rysy ve funkcích, vlastnostech nebo uživatelském rozhraní. Jedinou výraznou změnou byl restrukturalizovaný interní kód. Tím se dosáhlo použitelnosti pro operační systém Windows 3.0. [3, s. 22]

Verze 2.0

Druhá verze aplikace Notes přišla na trh v roce 1991. Firma Lotus se ve své obchodní politice vrátila k myšlence prodávat tento program se zaměřením na malé a střední podniky. Předchozí verze se prodávali hlavně do velkých nadnárodních korporací. Novinky v této verzi byly například Applications Programming Interface, možnost celkového sečtení hodnot ve sloupcích použitých v pohledech, nebo možnost vložení tabulek a formátování stylů. Tato verze byla první, která obsahovala podporu rich-textu a podporu více adresních knih. Umožňovala také přeposlání dokumentů v rámci poštovních služeb a nabízela funkci nastavení doručenky o přijetí poštovní zprávy příjemcem. Verze Lotus Notes 2.0 podporovala větší kapacitu databází a osobních souborů. Dále pak obsahovala rozšíření skriptovacího programovacího jazyka “*@Formula Language*”. [3, s. 22]

Verze 3.0

Lotus Notes 3.0 se objevila na trhu v květnu 1993. V této době už mělo aplikace Notes zakoupeno přes dva tisíce firem a jejich služby využívalo přes 500 000 uživatelů. Tato verze dále podporovala a rozvíjela klíčové funkce, pro něž byla aplikace Notes vytvořena. Jejím cílem bylo zejména vylepšit a zpříjemnit uživatelské prostřední interface a docílit rozšíření produktu na všechny známé platformy. A vytvořit tak z Lotus Notes takzvaný cross-platform product. Největší novinky této verze byly funkce pro fulltextové vyhledávání, hierarchická jména, selektivní replikace a replikace na

pozadí, podpora sítí AppleTalk, zvýšení výkonu, dostupnosti a stability systému a vylepšení nástrojů pro administraci systému. Klienta Lotus Notes bylo možné provozovat od této verze na i na operačním systému Macintosh a podpora serveru Lotus Notes se rozšířila o platformu Windows. Lotus SmartSuite byl v roce 1993 distribuován s bonus packem, který se nazýval „*Notes F/X*“. Tento bonus pack dovoloval aplikacím sdílet a integrovat data s Notes databázemi s využitím technologie Object Linking and Embedding. [3, s. 23]

Verze 4.0

V lednu roku 1996 se na trhu objevila již čtvrtá verze aplikace Lotus Notes. Přišla s kompletně upraveným designem uživatelského prostředí. To bylo založeno na informacích získaných od zákazníků a na jejich zpětné vazbě. Otevřená aplikace může od této verze nově obsahovat až tři panely, kterými jsou navigační panel, panel dokumentů a panel náhledu na dokument. Program Lotus Notes je rozšířen o záložku pro replikace. Novinky, které přinesla tato verze, se týkaly především integrace technologií Notes s webovými technologiemi. Jedním z těchto novinek byl nový prvek, který se jmenoval Server Web Navigátor. Ten dovoloval Notes serveru připojovat se na internet a tam pracovat s webovými stránkami. Webové schránky pak zpřístupnil uživatelům klientu Lotus Notes. Dalším příkladem sbližování obou technologií byl InterNotes Web Publisher. Web Publisher umožňoval transformaci Notes dokumentů do HTML a jejich následnou prezentaci na webu. Hlavní novinkou této verze bylo její rozšíření o další programovací jazyk LotusScript, který tak doplnil “*@Formula Language*”. [3, s. 24]

Verze 4.5

Roku 1996 přichází již firma IBM s další verzí aplikace Notes. Od této verze se také mění jméno Lotus Notes serveru na Domino 4.5 Powered by Notes. Jméno klienta zůstává stejné a to Lotus Notes 4.5 Klient. Velkou novinkou této verze byla transformace Domino serveru do interaktivního webového aplikačního serveru při zachování předchozích předností Notes serveru. Tento server dokázal kombinovat otevřené síťové prostředí internetových standardů a protokolů s velkou silou tvorby Notes aplikací. Domino také dále nabízelo možnost rychlé tvorby široké škály

obchodních řešení pro internet a intranet. Server umožňoval prezentovat Notes dokumenty v dynamickém procesu přímo na webu. K dalším novinkám patřily nativní kalendářové a plánovací funkce v rámci poštovních služeb, podpora SMTP/MIME, podpora POP3 na Domino serveru a podpora JAVA apletů, Netscape plug-in API a HTML 3.2. Tato verze rozšířila Access Control List o další oblast bezpečnosti Execution Control List a možnost nastavení periody pro vypršení platnosti hesla. Dále také přidala vlastnost, znemožňující opakované použití stejného hesla. Tato verze se v oblasti tvorby Notes aplikací rozšířila o podporu Java 1.1 a Java-base přístupu do objektů Notes. Nabízela také možnost skrývání libovolných elementů jak pro klienta Notes, tak pro klienta webového prohlížeče. [3, s. 25]

Verze 4.6

Verze 4.6 přišla na trh v září 1997. Jednalo se o verzi programu, která obsahovala již víc než pět a půl milionu řádků programového kódu. Novinky v této verzi byly zaměřeny hlavně na integraci soukromých informací a správu informací pocházejících z Notes aplikací a webových aplikací. Klient nově podporoval nové uživatelské rozhraní s názvem „Portfolio“. Tento klient tak mohl být poštovním klientem i jiných poštovních serverů díky POP3 a IMAP. Lotus Notes umožnil spuštění internetového prohlížeče přímo uvnitř programu a zvýšil interakci s produkty MS Office a Lotus SmartSuite. Domino server byl díky těmto vylepšením povýšen na standard pro Enterprise Messaging, Groupware a webové aplikační servery. Podporoval také protokoly LDAP, NNTP a zlepšil podporu HTTP a SSL protokolů. [3, s. 26]

Verze 5.0

Tato verze, která se vyznačovala integrací webu, se na trhu objevila na začátku roku 1999. Kód verze R5 byl přímým potomkem kódu verze R1 a části této architektury stále podporovaly i tuto novou verzi. Přes částečnou kompatibilitu se staršími verzemi byla verze R5 razantním krokem kupředu. Integrace webových a internetových technologií pokračovala na Notes klientovi a Domino serveru. Prostředí Notes klienta se začalo podobat rozhraní, které se zobrazovalo uživatelům ve webových prohlížečích. Lotus Notes klient tak získával charakteristické rysy a prvky prohlížečů. Verze Notes R5 samozřejmě podporovala víc internetových protokolů než předchozí verze. Rozšiřovala

možnosti přístupu do dalších datových úložišť jiných podnikových systémů, než byly Notes databáze. Klient pro vývojáře a programátory se v této verzi přejmenoval z Lotus Notes Designer na Domino Designer. Domino Designer byla aplikace, která byla integrovaným vývojovým prostředím s nástroji pro potřeby rychlého vývoje a nasazení bezpečných e-business aplikací na míru podniku. Třetí klient této série Domino Administrator umožňoval snadnější administraci prostředí Lotus Notes/Domino. Správu uživatelů a jejich účtu a nové nástroje pro monitoring serverů a management poštovních zpráv zajišťoval právě Domino Administrátor. Lotus Notes klient nabízel ve verzi R5 velmi snadný přístup do všech důležitých informací. A to osobních jako byly e-mail, adresář, kalendář a úkoly, tak i těch veřejných, v podobě oblíbených webových stránek, internetových diskusních skupin a knihoven dokumentů. Tato verze obsahovala v rámci nového rozhraní také volitelnou úvodní stránku. Na ní se mohli objevovat aktuální důležitý informace, ke kterým tak měli přístup všichni uživatelé. [3, s. 26]

Verze 6.0

Po třech letech od vydání úspěšné verze 5 se na trhu objevila v říjnu roku 2002 další nová verze Lotus Notes. Tato verze je charakteristická pro dobu, kdy dominovala témata kolem snižování nákladů, zvyšování produktivity, rychlejší implementace čehokoli a možnosti rychlé změny stavu, rychlého zvratu jakéhokoli rozhodnutí. Proto se verze R6 s aplikacemi Lotus Notes a Domino nesla na vlně požadovaného trendu a její charakteristikou tak bylo rychleji, lépe a levněji. [3, s. 28]

Verze 6.5

Hned rok po vydání verze 6.0 se v září 2003 objevila nová verze Lotus Notes/Domino 6.5. Tato verze nabízela především velmi úzkou integraci s technologiemi, mezi které patřily aplikace Sametime Instant Messaging, Domino Web Access, Lotus QuickPlace a Lotus Domino Dokument Manager. Verze 6.5 se tak stejně jako její předchůdce nesla v duchu charakteristiky „rychleji, lépe a levněji“. Tato verze byla rozšířena směrem ke komunikaci, a to komunikaci okamžité v režimu on-line. Hlavním rozšířením této verze byla integrace aplikace Sametime Instant Messaging do prostředí Lotus Notes/Domino. Díky tomuto rozšíření se mohl uživatel z klienta Notes 6.5 přihlásit k Sametime serveru, zjistit, kteří uživatelé jsou právě přihlášeni a začít s nimi chatovat. Uživatel tak mohl

realizovat on-line schůzky a chatovat s jedním nebo více uživateli naráz. Toto významné rozšíření funkcionality se od této verze stalo součástí prostředí Lotus Notes/Domino a bylo zahrnuto v jeho ceně. Další změnou bylo rozšíření funkcí v nástrojích kalendáře, plánování a pošty o možnost "drag and drop". Uživatel tak mohl například velmi snadno vytvořit záznam v kalendáři nebo nový úkol z poštovní zprávy pouhým uchopením a přetažením jakéhokoli e-mailu do záložky Kalendáře nebo Úkoly. Vše samozřejmě fungovalo i v opačném směru a tak mohl uživatel vkládat do e-mailů například odkazy k databázím pro další uživatele, kterým e-mail poslal. Uživatel také mohl vytvořit e-mail ze záznamu v kalendáři nebo úkolu. V poště se dále objevila možnost označovat zprávy pomocí značky ,,Folow Up". Tyto značky upozorňovali, že je v budoucnu potřeba provést s dotyčnou zprávou nějakou aktivitu, tedy poštu vyřídit. Dalším z mnohých vylepšení této verze byla možnost snadno určit, které e-maily budou automaticky uloženy do pořadače nevyžádané pošty. Pro nevyžádanou poštu byla v Notes zřízena složka označená jako Junk Mail. Uživatel tak mohl v této verzi velmi snadno vytvořit pravidlo, kterým do této složky přesměroval veškerý spam. Došlo také k vylepšení výkonnosti Domino serveru. Výkonnost je důležitým prvkem prostředí klient/server. Souběžně s vylepšením výkonnosti se vylepšily i některé další funkce v prostředí administrace Domino serverů a Domino domén s důrazem na platformu Linux. [3, s. 28]

Verze 7.0

Verze 7 se i nadále soustřeďovala na zlepšování spolupráce, zvyšování produktivity a plynulost obchodních procesů. Společnost IBM s Lotus Notes 7 a serverem Domino stejné verze pokračovala v nabídce prvků potřebných k maximalizaci spolupráce a interakce s člověkem. Toto napomohlo ke snížení celkových nákladů na vlastnictví. Tato verze přišla s plnohodnotným zabezpečením, rozšiřitelností, spravovatelností, produktivitou, znovupoužitelností a tvárností. Lotus Notes a Domino 7 nabízí výkonné schopnosti zasílání zpráv a spolupráce. Produkty Lotus Notes a Domino 7 napomáhali při zvyšování produktivity organizace. IBM nabídl v této verzi některá vylepšení a mnoho novinek, které umožnili lépe provádět každodenní úlohy a aktivity. Jsou to pracovní plocha, úvodní stránka, moje pracovní úkoly, kalendář, adresní kniha a odesílání okamžitých zpráv. Verze 7 také zajistila důležité funkce a základní pilíře

podniku jako jsou zlepšený výkon serveru a jeho rozšiřitelnost podporuje více uživatelů s využitím nižšího počtu prostředků, zabezpečení a administrativní řízení podporující plnohodnotný systém zpráv v rámci celého podniku a řešení pro spolupráci, lepší účinnost z pohledu uživatele, zdokonalené funkce pro zvýšení produktivity. Dále pak nové nástroje pro správu a podporu starších verzí. [5]

Verze 8.0

14. června 2005 představil generální manager IBM další verzi Lotus Notes. Její kódové jméno bylo „Hannover“. Novinky, které tato verze přinesla, byla především vylepšená komprese databází. Například u poštovních databází se díky této kompresi ušetří až kolem 40 procent místa na disku. Další novinkou je nativní podpora 64bit pro Windows 2003, úplně nový Domino Web Access (iNotes), sekundární kalendář a časové zóny, grafické zobrazení kvóty mailu přímo ve schránce, podpora klientů na Citrusu a integrace Widgets. Velkou novinkou je také Lotus Notes Traveler, který zajistí napojení Notes dat na mobilní zařízení. Traveler podporuje Windows Mobile 5.0, Windows Mobile 6.0 i BlackBerry. [3, s. 32]

Verze 8.5

Tato verze přináší atraktivní vzhled podobný standardu MS Outlook. Oblíbené funkce a aplikace je možno uživatelsky integrovat do bočních lišt a lepší správu kontaktů. Informace o odesílateli/adresátu se objeví po najetí myši. Jednou z novinek této verze je i “našeptávač”. Díky němu se odesílatelé automaticky ukládají do adresáře a sami se po zadání prvních několika písmen ze začátku jména nabízí při dalším odesílání. Menu je obecně jednodušší a pro uživatele přátelské. Od verze 8.0 je součástí Lotus Notes i aplikace Lotus Traveler umožňující synchronizaci pošty s mobilním telefonem obdobně jako BlackBerry. Výhodou je širší podpora mobilních zařízení a také, že klient Lotus Traveler je zdarma součástí verze 8.5. Velice dobře funguje integrace sametime klienta s vylepšenou správou kontaktů. Tato verze přináší i nové provedení kalendáře, jeho sdílení a barevné zobrazení v něm. Další novinkou je integrace WWW stránek do widgetů, uživatel tak má požadované weby neustále po ruce. Webová šablona pošty, obecně web access je velmi zdařilý. Obsahuje 3 různé pohledy podle „kvality“ zobrazení, které je možno zvolit dle rychlosti připojení. Všechny aplikace doposud

používané jsou i nadále plně funkční. Velice dobře funguje synchronizace lokálních kontaktů s kontakty ve webové šabloně, lze pak využít při napojení na BlackBerry či Lotus Traveler. Další novinkou je Lotus Symphony. Jedná se o poměrně zdařilou alternativu k MS Office, která je integrovaná do klienta. [11]

3.2 Mobilní použití a replikace

Mobilním použitím se rozumí užívání klientu Lotus Notes bez připojení k sítí či internetu. Mobilní užití je tedy převážně z notebooku například doma, na chatě nebo ve vlaku. Uživatel aplikace Lotus Notes tak pracuje s programem ve více typech pracovišť, která jsou různě nastavená. V případě, že uživatel není připojen, užije předvolené pracoviště „Ostrov“, které je nastaveno na lokální použití. Jde většinou o uživatele s notebookem nebo jiným přenosným počítačem. Druhé pracoviště „Kancelář“ je nastaveno klasicky a volí ho při příchodu do firmy, nebo pokud má přístup k internetu. Uživatel tak přepíná tato pracoviště, protože jednou pracuje s Lotus Notes klientem ve své kanceláři, kdy je k domovskému a poštovnímu Lotus Domino serveru připojen on-line pomocí lokální sítě a protokolu TCP/IP a aplikacemi a databázemi pracuje přímo na serveru. V druhém případě pracuje s klientem doma v režimu off-line, to znamená, že není připojen k domovskému Lotus Domino serveru a pracuje s replikami a kopiemi databází a aplikací, které musí mít pro tento případ zreplikované ve svém notebooku. Uživatel tak pracuje s poštou a aplikacemi normálním způsobem i bez připojení k síti. Poté co má práci hotovou, například nové poštovní zprávy a odpovědi na došlé zprávy, zpracované informace ze schůzek, nebo vypracované úkoly v aplikacích. Může se připojit na domovský a poštovní Lotus Domino server internetu, nebo v případě, že se jedná o zabezpečenou firemní sít, použije k připojení VPN klienta. Následně provede odeslání připravené pošty a replikaci poštovní databáze a databáze, která obsahuje informace ze schůzek. Tím se provede synchronizace údajů mezi Notes aplikacemi na Lotus Domino serveru a jejich replikami, které jsou umístěné na lokálním disku uživatele. Jak již bylo zmíněno, aby uživatel mohl pracovat v off-line režimu s databázemi a aplikacemi, musí si vytvořit repliky všech aplikací a databází, které ke své práci potřebuje. Minimálně je třeba vytvořit kopii poštovní schránky k možnosti práce s poštou off-line. Vhodná je i aktualizovaná replika adresní knihy s adresami vhodnými pro práci.

Replika Notes databáze je kopie databáze se stejným ID repliky jako má původní databáze, která je většinou uložená na serveru. ID repliky je jedinečné a jednoznačné hexadecimální číslo Notes databáze, které nalezneme ve vlastnostech databáze v záložce Informace (*File – Database - Properties – Info – Replica ID*). Od verze Lotus Notes 8 je v menu File, nahrazena záložka Database záložkou Application. Aplikace Lotus Notes umožňuje vytvářet repliku databáze z libovolné databáze či aplikace, kterou používáme na Lotus Domino serveru, do Lotus Notes klienta. Pomocí vhodného nastavení replikací se může zajistit, aby byla lokální replika databáze identická s Notes databází na serveru. Znamená to, že se provedené změny v jedné z Notes databází projeví po jejich replikaci ve všech jejích replikách na všech serverech. Replikace tedy zajišťuje synchronizaci všech replik Notes databází. A tím zajišťuje jejich identičnost. Jelikož je práce s lokální replikou Notes aplikace mnohem rychlejší než provádění stejných změn pomocí telefonického připojení nebo pomalého WAN připojení na Notes aplikaci uložené na Lotus Domino serveru, představuje replikace výkonný nástroj především v případě, kdy nepracujeme v lokální síti naší společnosti.

Záložka Replikace v klientu Lotus Notes slouží ke správě a nastavení replikací. K ručnímu ovládání replikace jako je spouštění, zastavování a zobrazení všech replik Notes aplikací, které jsme si vytvořili. Replikaci můžeme naplánovat, aby se spouštěla periodicky v požadovaný čas. Je vhodné nastavit replikace vždy při spuštění klienta a připojení na server a také při ukončování klienta. V případě, že chceme, aby se změny projevili ihned po provedených změnách na všech serverech, je možné replikaci spustit ručně. Pro každé pracoviště, které v aplikaci Lotus Notes používáme, můžeme nastavit jiný plán replikací.

Je možné spravovat replikaci všech lokálních Notes databází. Můžeme snadno replikovat jednu nebo více databází s jedním nebo více servery a v průběhu tohoto procesu replikace v aplikaci Lotus Notes pokračovat nerušeně v další práci, jelikož replikace běží na pozadí a další práci s databází nijak neomezuje. [3, s. 185]

3.3 Bezpečnost systému

Díky současnému zabezpečení aplikace Lotus Notes je možno na vysoké úrovni chránit pracovní plochu uživatele klienta Lotus Notes a informace, jako jsou data uložená lokálně i na Lotus Domino serveru, s kterými uživatel pracuje. Díky kvalitnímu zabezpečení je tak zajištěno, že k informacím má přístup vždy oprávněná osoba, které naše informace a data zpřístupníme. K přihlášení do aplikace Lotus Notes je možné mimo standardního přihlašování použít i kartu Smartcard. Na této kartě můžeme také uložit své soukromé klíče do internetu. Administrátoři mohou snadno obnovit uživatelské ID v případě ztráty karty Smartcard. K dalšímu zabezpečení pošty můžeme použít certifikáty aplikace Lotus Notes a sítě Internet, tím se zabrání nepovolaným osobám číst naše odeslané a přijímané poštovní zprávy. K ujištění příjemce o pravosti odesílatele je možné připojit ke zprávě digitální podpis. Tím snadno prokážeme, že odesilatelem jsme my a nikoli jiná osoba. Dále je možné v aplikaci Lotus Notes nastavit tak lokální šifrování pro všechny nové repliky Notes aplikací, které vytvoříme. Můžeme zašifrovat také všechny vytvořené dokumenty, takže je budou moci přečíst pouze osoby, kterým nastavíme přístup v ACL této databáze nebo aplikace. Můžeme také nastavit omezení činností, jež mohou uživatelé provádět v našem klientovi, a nastavit přístupová práva v ACL našich databází a aplikaci, nebo v těch kde jsme manager. [3, s. 223]

3.3.1 Autentizace

Po spuštění klienta je první, s čím přijde uživatel do styku autentizace. Autentizace je jednoznačná identifikace uživatele, který se chce přihlásit na poštovní server. Server, na který se uživatel přihlašuje, je nastaven při instalaci klienta Lotus Notes. Klient Lotus Notes představil pro autentizaci uživatele přístup, který byl ve své době celkem revoluční. Jednalo se o to, že identifikace uživatele byla nejen na základě klasického přístupového hesla, ale i na základě takzvaného Notes ID. Notes ID je něco jako elektronický průkaz, reprezentovaný souborem velikosti několika málo kB na pevném disku, USB flash disku nebo jiném médiu. Tento soubor je nutné mít při ruce vždy, když se chce uživatel přihlásit do klienta Lotus Notes a pracovat sním. [1, 14]

Ke každému přihlášení do aplikace Lotus Notes klienta je tedy třeba již zmíněný ID soubor uživatele. ID je soubor, který byl vytvořen správcem systému při vytváření

uživatelského účtu. Toto ID obsahuje informace, které aplikace Lotus Notes slouží k identifikaci uživatele v systému a je vněm také uloženo a zašifrováno heslo uživatele pro vstup do klienta. Soubor ID je obvykle uložen v adresáři Notes\Data a lze jej rozpoznat podle přípony ID, například "jrichtr.ID". Jelikož ID uživatele slouží k identifikaci naší osoby při přihlašování, je potřeba jej uložit na bezpečeném místě, jako by šlo o jakýkoli jiný osobní dokument naší totožnosti. A to i přesto že je chráněn heslem a zašifrován. Vhodné je uložit kopii ID uživatele na pevný disk lokálního počítače či notebooku a další kopii na jiný paměťový nosič. Ten je dobré uložit na bezpečeném místě. Tím si zajistíme, že budeme mít pro případ nouze další záložní kopii našeho USER ID. Díky USER ID, se můžeme přihlašovat do libovolného klienta na jakémkoli počítači, kde je nainstalovaný. Pro tento způsob je však vhodné mít ID uložené například z flash disku a z něj do klienta přistupovat. V případě, že nahrajeme ID na lokální disk počítače, je z bezpečnostních důvodů vhodné ho po dokončení práce odstranit.

Pokud máme multiuživatelské nastavení Lotus Notes a sdílíme počítač s dalšími uživateli nebo sami používáme více než jedno ID uživatele, můžeme libovolně přepínat mezi jednotlivými uživatelskými ID a to například v případě, když chceme získat přístup k poštovnímu Domino serveru nebo jiným Notes aplikacím. Abychom mohli přepnout mezi ID soubory uživatelů, musíme být ID soubory dostupné. Pro každé ID je nutné nastavit zvláštní pracoviště. Tím je pak možné přepínat mezi účty přímo v klientu bez jeho restartu jen na základě změny pracoviště. Pracoviště je pak vhodné k snadné identifikaci dobře pojmenovat.

V případě odchodu od počítače je vždy vhodné zamknout zobrazení aplikace Lotus Notes, abychom ochránili informace, ke kterým máme přístup pomocí svého USER ID. To docílíme například stisknutím klávesy F5 při odchodu z pracoviště. Dále je možné nastavit přímo v klientu automatické zamykání po určitém časovém intervalu, kdy je klient nečinný. [3, s. 224]

3.3.2 Autorizace

Po úspěšné autentizaci přichází na řadu autorizace. Po úspěšném zadání hesla tedy již server Domino ví, s kým komunikuje a zná jeho přesnou identitu, nicméně v dalších krocích musí rozhodnout, jaké operace může tento uživatel provádět a s jakými dokumenty bude moci pracovat. Celý proces autorizace se řeší na několika vrstvách.

První z vrstev kontroluje, kteří uživatelé či skupiny uživatelů mohou vůbec na server přistupovat. V případě, že je uživatel například uveden mezi zakázanými lidmi ve skupině DenyAccess, nebo naopak není uveden ve skupině mezi uživateli s povoleným přístupem, server Domino jej nepustí dál ke svým databázím a zahlásí mu nedostatečná přístupová práva na server. Tím je uživateli znemožněna práce on-line na serveru a může pracovat s klientem pouze v off-line módu.

Druhá vrstva představuje nastavení Access Control Listu u jednotlivých databází v Lotus Notes. V seznamu přístupových práv ACL, který umožňuje přehledně a intuitivně škálovat rozdělení oprávnění s velkou volností, nastavíme požadovaná práva pro jednotlivé uživatele, skupiny uživatelů či serverů.

Třetí vrstva představuje možnost nastavení čtecích či editační práva přímo k jednotlivým dokumentům uložených v databázi, nebo dokonce pouze k vybraným částem v dokumentech či sekcím databází. Například v personální databázi se běžným firemním uživatelům přidělí práva autorská. To znamená, že tito uživatelé číst záznamy ostatních uživatelů a každý z nich může libovolně měnit a aktualizovat svůj záznam v adresní knize nebo databázi. U každého dokumentu je však možné nastavit část veřejnou, ke které budou mít přístup všichni tito uživatelé a také část neveřejnou do které bude mít přístup pouze vlastník a vyvolená skupina administrátorů. Tím zabezpečíme ochranu citlivých osobních údajů jednotlivých uživatelů. Veškeré údaje tedy jsou v jednom dokumentu, ale my můžeme nastavit přístupová práva tak, aby každý uživatel viděl to, co mu náleží a na co má pravomoc. [14]

Jak již bylo zmíněno, převážná většina nastavení ohledně autorizace uživatelů se provádí v Access Control Listu. Nastavení ACL patří mezi základní znalosti každého administrátora Lotus Notes a ovládat jeho základy by měl i každý uživatel. Tato činnost se provozuje zejména při zakládání nových databází, nastavování nového serveru, při tvorbě nových uživatelských skupin, nebo při delegování přístupových práv dalším uživatelům.

Každá databáze má v Lotus Notes svůj vlastní Access Control List. Každá databáze však může mít na různých serverech, nebo lokálních discích uživatelů, více svých replik, které se pravidelně synchronizují. Je proto důležité nastavit průběžnou synchronizaci nastavení ACL i do všech replik. Tato situace je ideální pro celkovou správu databází. V případě speciálních řešení je však možné tuto vlastnost zakázat a mít na každé replice nastaveno ACL jinak dle aktuální potřeby.

Systém kontroluje při každém pokusu o přístup uživatele nebo serveru k databázi, zdali mu nastavení Access Control Listu povolí tuto databázi otevřít. Do rozhraní ACL databáze se můžeme dostat několika způsoby. Pokud je databáze otevřena je možné vybrat z menu *File* - *Application* - *Access Control*. Druhým způsobem je otevření pracovní plochy a zde je možno pravým tlačítkem myši zvolit nastavení Access Control. Po vstupu do Access Control se objeví okno s aktuálním nastavením přístupových práv. Pokud má uživatel dostatečná přístupová práva, může nastavení ACL libovolně měnit. Pokud nebude mít dostatečné oprávnění, bude mít tlačítka zašedlé a nebude moci s ACL pracovat. Okno s nastavením ACL se na první pohled může zdát složité a nepřehledné, jelikož obsahuje všechno potřebné nastavení. Práce s ním je ale velmi jednoduchá a intuitivní. Na levé straně jsou 4 záložky, pomocí nichž je možné přepínat mezi jednotlivými sekcemi ACL. Hlavní a nejdůležitější je v rozhraní ACL první záložka Basics. Její největší část zabírá sekce uprostřed s názvem Access Control List. Ta obsahuje seznam uživatelů, serverů a skupin. Při kliknutí myší na jméno se změní zaškrtnutí políček v pravém sloupci atributů. Pravý sloupec Attributes je totiž to místo, kde je možno nastavit uživatelům, serverům či skupinám vhodná práva k databázi. Pravý sloupec se dělí na tři základní části. Vrchní část nastavuje typ entity a základní úroveň přístupu uživatele. Prostřední část osahuje devět checkboxů, ve starších verzích

Lotus Notes se můžete setkat i s menším počtem checkboxů, určených pro přesnější a jemnější přidělování jednotlivých práv. Ve spodní části se nachází sekce Roles. Zde je možno nastavit uživatelské role, které umožní provázat ACL s prvky návrhu nebo se sadou dokumentů v databázi Lotus Notes.

Klíčovým sloupcem v ACL je právě již zmíněný sloupec Attributes, který leží na pravé straně. Je zde možno vybrat až ze šesti předem definovaných profilů. Mezi ně patří: Unspecified, Person, Server, Mixed group, Person group a Server group. Toto nastavení je velice důležité, nesprávnou volbou může dojít k nechtěnému odříznutí vybrané skupiny či uživatele od přístupu k celé databázi.

Přehled možných profilů:

- **Person a Server:** Tyto dvě entity mohou k databázi přistupovat jak uživatelsky, z klienta Lotus Notes, nebo serverově, při komunikaci dvou serverů mezi sebou. Pro uživatele se tedy nastavuje typ Person a pro servery typ Server. Pokud přidělíme uživateli typ Server, k databázi se nedostane, protože k němu bude přistupovat uživatelským způsobem, ale má povolen pouze serverový přístup. To samé platí i naopak.
- **Person group a Server group:** Jedná se o varianty pro skupiny uživatelů, nebo skupiny serverů. Pokud se nastavuje přístup do databáze pro skupinu uživatelů či skupinu serverů, vybereme tyto typy.
- **Unspecified a Mixed group:** Poslední dvě entity jsou varianty, kdy dopředu nevíme, jakého typu bude nebo je daná entitia. Jako Unspecified se dá označit každá entita, které bude povolen přístup jak uživatelský, tak serverový přístup k databázi. Profil Mixed group popisuje skupinu, kde jsou jak uživatelé, tak servery dohromady. Může se například jednat o skupinu se všemi uživateli a servery v celé společnosti.

Základní úrovně přístupu:

- **No Access** - Bez přístupu. Tato entita nemá přístup k databázi. Použít tuto úroveň přístupu má smysl například tehdy, pokud uživatel je členem skupiny, která má práva přístupu k databázi, ale přímo jemu chceme nějaká práva, které má skupina odebrat.
- **Depositor** - Vkladatel. Jedná se o zvláštní úroveň přístupu, kdy má daná entita právo zapisovat do databáze, ale nemá právo z databáze nic číst. Dá se to přirovnat k poštovní schránce, do které lze pouze házet dopisy. Příkladem nejčastějšího použití této úrovně je databáze mail.box, která se nachází na každém serveru. Tato databáze slouží jako fronta pro maily čekající na odeslání. Každý uživatel do ní může zapisovat, nebilo přidat mail k odeslání, ale číst v ní mohou jenom administrátoři a server.
- **Reader** - Čtenář. Uživatel s touto úrovní přístupu může číst dokumenty. Nemůže je však mazat ani vytvářet.
- **Author** - Autor. Entita má práva pro čtení a navíc může i vytvářet nové dokumenty. Dokumenty co vytvoří, může následně upravovat, případně mazat. Tento typ přístup se nejčastěji užívá stejně jako Reader pro běžné uživatele. Proto pro něj dále existuje řada možností, jak blíže specifikovat. Například které dokumenty může upravovat a zda je může mazat.
- **Editor** - Editor. Úroveň přístupu určená pro uživatele, kteří za obsah databáze určitým způsobem odpovídají. Tito uživatelé mají stejná práva jako Autoři. Jedinou odlišností je, že mohou navíc upravovat i mazat dokumenty, které vytvořili ostatní uživatelé.
- **Designer** - Návrhář. Určeno pro vývojáře, programátory, designery, kteří mají stejná práva jako Editoři. Designéři však mohou i vytvářet či měnit design databází a upravovat jejich systémové vlastnosti.
- **Manager** - Manažer. Tato skupina je určena pro správce systému Lotus Notes. Manažeři mají stejná práva jako Návrháři, ale navíc mohou nastavovat přístupová práva pro ostatní. Dále pak mohou nastavovat všechny systémové vlastnosti databáze a mohou databázi ze serveru smazat. Každá databáze musí mít aspoň jednoho Manažera, aby ji bylo možné spravovat.

Při přepínání předchozích sedmi úrovních přístupu se dle vlastností mění i zvolené checkboxy. Těchto devět checkboxů je přímo navázáno na úrovně přístupu a umožňují také přidat nebo ubrat další privilegia a tím upřesnit nastavení přístupu. Každá úroveň nabídne k zaškrtnutí jinou množinu checkboxů. Tato vlastnost je natavena proto, že například pro úroveň Reader nelze vybrat možnost Delete document, ale pro úroveň Editor již ano.

Popisy checkboxů:

- **Create documents** – Tento checkbox umožňuje vytvářet dokumenty. Skupiny úrovně přístupů nedávají automaticky právo tvořit dokumenty, ale pouze nabídnou možnost zvolit tento checkbox a tím toto právo přiřadit.
- **Delete documents** – Entita, která má toto právo může mazat dokumenty. Z bezpečnostních důvodů je to vypnuto defautlně pro všechny úrovně přístupu. Dokonce i Manager si musí dodatečně zaškrtnout právo mazání dokumentů.
- **Create Private Views** – Každý uživatel s tímto oprávněním může vytvořit vlastní pohled na data. Pohled je následně uložen na lokálním disku počítače uživatele v souboru desktop8.ndk.
- **Create personal folders/views** - Uživatel může díky této pravomoci vytvořit vlastní pohled či složku uloženou na serverové replice databáze. Tuto repliku nevidí ostatní uživatelé. Tato možnost je vhodná zejména v případě, kdy uživatel potřebuje mít pohled na data, který nebyl vývojáři databázi vytvořen.
- **Create shared folders/views** – Toto právo umožňuje uživateli vytvářet a upravovat sdílené pohledy a složky i přesto, že není jejich autorem. Toto právo se doporučuje všem běžným uživatelům defaultně vypínat, pokud není jiný důvod k jeho aktivaci.
- **Create LotusScript/Java agents** – Užitečné pravidlo, bez kterého by uživatelé nemohli využívat některých funkcí Lotus Notes, jako je například možnost nastavit agenta Mimo kancelář, který na každý doručený e-mail odešle informaci o nepřítomnosti příjemce. Pomocí agentů se také řídí také pravidla nastavená v poštovní schránce. Agent je skript, který se spouští automaticky v pravidelných intervalech nebo na vyžádání uživatele. Uživatel si může vytvořit

například ve své poštovní databázi agenta, který všechny maily s určitým parametrem přepošle na jeho mobil jako SMS. Je nutno splnit ovšem ještě druhou část administrátor musí tomuto uživateli dát právo spouštět agenty na serveru.

- **Read public documents** – Právo, které je podobné například No Access a Reader. Toto oprávnění se využívá například při zpřístupnění poštovní databáze kolegům. Nastavíte-li jim profil No Access a přidáte právo Read public documents, tak kolegové získají oprávnění vidět váš kalendář a vaše úkoly. To však kromě položek, které jste označili jako soukromé.
- **Write public documents** – Obdobné oprávnění jako Read public documents, jenom navíc s možností veřejné dokumenty vytvářet a také editovat.
- **Replicate or copy documents** – Opět jedno z důležitých práv. Pokud entitita toto právo nemá, může obsah databáze pouze číst, ale nemůže tuto databázi replikovat a nemůže dokumenty z databáze kopírovat do jiné databáze a to dokonce ani jejich části.

Samotné entitiy do ACL můžeme přidat či odebrat pomocí tlačítek Add, Rename, Remove. Tlačítkem Add lze přidat uživatele, server či skupinu. Platí u toho jedno pravidlo, že nově přidávaná entita dostane zpočátku stejná práva, jako má ta, která je právě zvolena. Nejjednodušší postup při přidávání dalšího uživatele do databáze, je ten, kdy si myší vyberete již existujícího uživatele v ACL, který má stejná nebo velmi podobná práva, jaká má mít i nový uživatel a potom dole zvolíte Add a doplníte pouze jiné jméno nového člověka. Následně je vhodné skontrovat v pravém sloupci, jestli je vše pořádku a případně upravit nastavení dle potřeby. Tlačítkem Remove se odstraní aktuálně vybraná entita z celého ACL. Nelze však odstranit Manažera databáze pokud je zde jen jediný. Tlačítko Rename slouží k přejmenování zvolené entity.

V Access Control Listu každé Notes databáze je vždy položka Default. Tu nikdy nelze smazat a slouží k výchozímu nastavení přístupu k databázi v případě, že uživatel není uveden v ACL explicitně ani skrze členství v žádné skupině. Pro většinu databází by mělo být Default standardně nastaveno na No Access. Vyšší práva přidělujte potom

pomocí dalších uživatelských skupin. Default se vztahuje na ty přístupy, které jsou autentikované. To jsou přístupy, kde je známa identita přistupujícího uživatele či serveru. Mohou zde ovšem nastat situace, kdy tato identita známa není. To může nastat v případě, že je databáze zpřístupněná přes webové rozhraní i pro anonymní uživatele. V tomto případě je možné použít další systémovou entitu Anonymous. Entita Anonymus se aplikuje tehdy, když identita přistupujícího není známa a to zpravidla když se jedná o přístup k databázi anonymně přes webový prohlížeč. Zde by tak měla být nastavena ještě slabší práva, než má entitia Default.

Seznam oprávnění k databázi, neboli Access Control List doplňuje Execution Control List. ECL je seznam oprávnění spouštět operace v klientu Lotus Notes. Každý kousek kódu, který je v Lotus Notes vytvořen, je digitálně podepsán svým autorem, nebo tím, kdo jej naposledy editoval. Do ECL je tedy z bezpečnostních důvodů vhodné zanést pouze ta jména vývojářů, a hlavních administrátorů. Pokud na pracovní stanici spustí uživatel kód, jehož autor nemá oprávnění v ECL, objeví se nejdříve varující dialog, ve kterém je možné podezřelou operaci povolit nebo zakázat. Tato funkcionalita úspěšně zamezuje šíření škodlivých samospouštěcích skriptů. Díky Execution Control Listi se tak tento škodlivý kód nemůže spustit a způsobit tak problémy. [15]

Pod záložkou Basic se v levém panelu ACL nachází záložka Roles. Role umožňují provázat ACL s prvky návrhu nebo se sadou dokumentů v databázi. Záložka Roles v dialogovém okně ACL slouží právě pro vytváření těchto rolí. Role v ACL jako taková je pouze pojmenování. Pro aktivaci role je nutno ji provázat na více místech včetně návrhu databáze.

V ACL se role vytvořené v sekci Roles se ihned objeví v pravém dolním rohu sekce Basics. Zde můžete prostým zaškrtnutím checkboxů přidělovat role jednotlivým subjektům jako jsou uživatelé, servery čí skupiny uživatelů, nebo skupiny serverů. Žádná role není přidělena žádnému subjektu defaultně. Všem uživatelům se role musí nastavovat manuálně.

V návrhu databáze je možné nastavit, jak se mají role chovat a co pro entitu znamená mít konkrétní roli. Designéři mají různé možnosti, jak role při programování aplikací využít. Pole čtenáři a autoři ve formuláři je pole typu čtenáři nebo autoři, které je již předvyplněno hodnotou. A to například jménem jedné nebo několika rolí. Jakmile se pomocí formuláře vytvoří dokument, bude se přístup k němu se řídit podle těchto předem nastavených rolí.

V případě, že je nežádoucí, aby některé ovládací prvky viděli všichni uživatelé, je možné ovládací prvky skrýt pomocí rolí. Do vlastnosti příslušného tlačítka, akce či sekce dokumentu se nastaví v aktivní položka „Hide when“. Tato položka zjistí, zda uživatel má či nemá příslušnou roli.

Třetí záložkou v ACL je Log. Je dobré evidovat veškeré dění v ACL a tím případně ihned zjistit kdo za jaké změny zodpovídá. Proto se každá změna v ACL zaznamenává do logů. V této třetí záložce Logs je tak možno vidět všechny zásahy a změny v přístupových právech dané databáze. Jsou tam zaneseny jak přidávání nových položek, tak veškeré updaty a změny nastavení a samozřejmě i evidence mazání položek. V případě problémů lze tak jednoduše dohledat, kdo je zodpovědný za špatně nastavenou položku v Access Control Listu.

Čtvrtou a zároveň poslední záložkou v ACL rozhraní je záložka Acvanced. V této záložce je možné provést systémová nastavení. Lze zde například nastavit, zdali se bude replikovat ACL spolu s databází na ostatní servery či nikoli. Toto lze také nastavit přímo pro vybrané servery. Lze zde také nastavit administrační server, možnost uzamčení ACL či nastavení hromadných změn v ACL. Administrační server je server, který se o danou databázi stará. Zároveň to musí být takový server, na němž se nachází alespoň jedna replika databáze. Pojem administrační server je propojen s procesem administrace, což je jedna z úloh serveru Domino, která má na starosti automatizované změny v databázích. Administrační server se dále například stará se o přejmenování uživatelů. V případě, že se uživatelka vdá, stačí pouze na jednom místě napsat její nové příjmení a administrační proces sám projde příslušné záznamy, databáze, ACL a podobně a zreplikuje její příjmení automaticky na všechy servery a do všech databází

kde uživatelka byla uvedena. Tyto příkazy automatické změny se se replikují napříč doménou přes všechny její Domino servery. Z dohotu důvodu je nutné zajistit, aby se o každou databázi staral nějaký server. Z toho předpokladu také vyplývá, že dvě repliky jedné databáze umístěné na dvou různých Domino serverech musí mít vždy tentýž administrační server. V případě, že by každou databázi spravoval jiný server, došlo by k dvojímu přejmenování a při první vzájemné replikaci by se objevily replikační konflikty. V záložce Advanced je dále možno nastavit jméno administračního serveru. Vybraný server se objeví v první záložce jako Manager a v ikoně bude mít symbol klíče. V řádku pod jménem serveru nazvaném Action se anstavuje pravomoc pro server, která obsahuje informace o tom, co všechno může administrační server v databázi měnit. Toto nastavení se týká již zmíněného automatického přejmenování polí, například při změnách příjmení vdaných dam.

Možné volby záložky Action u administračního serveru:

- **Do not modify Names fields**. Tato volba zajistí, že administrační server nebude měnit žádná políčka. Změna příjmení uživatelky se tedy do této databáze při tomto nastavení nepromítne.
- **Modify all Reades and Authors fields**. V případě volby toho nastavení bude administrační server měnit hodnoty pouze v polích typu čtenáři a autoři. Jedná se o systémová pole, pomocí kterých se nastavuje přístup k dokumentu v databázi.
- **Modify all Names fields**. Díky tomuto nastavení bude administrační server měnit hodnoty v polích. Změny se projeví u uživatelů s právy Reader a Autor a také v ostatních polích typu Names.

Další možností, kterou lze v záložce Advanced nastavit je Enforce a consitent Access Control List across all replicas. Toto se zkráceně nazývá zamknutí Access Control Listu, nebo také vynucení neměnného ACL. ACL z principu umožňuje mít na různých replikách jedné databáze různé nastavení ACL. To může být v určitých situacích výhodné. Pokud však správce databáze nechce, aby mu například lokální administrátoři na jiných pobočkách, kam se databáze replikuje, ACL měnil, zaškrtne tento checkboxů,

který mu tuto vlastnost zajistí. Při replikaci se potom zkontroluje, zda ACL je na obou stranách stejné. Pokud není, tak se replikace přeruší a do logu se zapíše, že někdo manipuloval s ACL databází na vzdáleném serveru. K databázi se dá přistupovat jak ze standardního klienta Lotus Notes, tak z webového rozhraní v podobě podporovaného internetového prohlížeče. ACL nastavuje práva pro oba tyto přístupy současně. Protože je ale přístup přes web obecně méně bezpečný, jelikož se při přihlašování nepoužívá soubor Notes.ID, ale pouze přihlašovací jméno a heslo, může správce databáze přístup z webu omezit. Pro možnost tohoto omezení je zde pole Maximum Internet name and password toto pole nabízí na výběr všech sedm úrovní. Vybraná úroveň potom slouží jako maximální pro přístup z webu. Defaultně je nastaven Editor, což je univerzální volba pro toto nastavení. Administrátor si ale může dle vlastního uvážení zvolit, co požaduje. [16]

3.3.3 Protokoly

Klient Lotus Notes a server Domino spolu komunikují pomocí vnitřního protokolu, který se stará o zabezpečené spojení mezi nimi. Server využívá pro komunikaci pouze portu číslo 1352, takže při nastavení firemního firewallu stačí povolit pouze tento port. Pokud se tak uživatelé aplikace Lotus Notes chtějí připojovat k serveru zvenčí, je nutné mít tento port povolen. Tuto komunikaci mezi klientem a serverem, která by se neodehrávala pouze v rámci firemní sítě lze navíc i šifrovat. Případný útočník, zachytávající komunikaci, tak získá pouze šifrovaná data, které nedešifruje. Lotus Notes umožňují uživatelům také pracovat off-line a to díky možnosti replikace. Replikace je vysoce sofistikovaná synchronizace, díky které lze uložit dokumenty v databázi i lokálně na pevný disk notebooku a při každém připojení k sítí je aktualizovat. S replikou databáze lze pak pracovat stejně, jako by byla na serveru, protože změny, které jsme v režimu off-line provedli, se po připojení do sítě vždy vyreplikují na server, a naopak. V případě, že dojde ke změnám jak na lokálním disku, tak na serveru u stejné položky dojde k replikačnímu konfliktu a replikace neproběhne. Veškeré databáze na lokálním disku je nutné šifrovat, aby se při jejich odcizení nedostali do nepovolaných rukou. Pokud však pro lokální repliky nastavíme šifrování, nikdo je bez souboru ID, kterým byly zašifrovány, neotevře. [14]

3.3.4 Standardy

Server Lotus Domino podporuje hned několik standardů. Mezi tyto standardy patří například skupina bezpečnostních standardů. Do této skupiny patří například standard S/MIME, který zajišťuje možnost odesílat a přijímat elektronicky podepsanou či šifrovanou poštu. Dále jsou to pak standardy pro podporu X.509 certifikátů a PKI. Soukromý a veřejný klíč si tak lze nechat certifikovat u externí certifikační autority.

Zabezpečení internetové komunikaci se serverem Domino, lze udělat i tak, že Lotus Domino bude sloužit jako registrační i certifikační autorita pro vydávání X.509 certifikátů, pomocí nichž se šifruje například HTTP protokol na HTTPS. [14]

3.3.5 Specifické bezpečnostní požadavky

V Lotus Notes je možné aplikovat i specifické požadavky na vyšší bezpečnostní kriteria. Je možné nastavit USER.ID tak, že ho neodemkne pouze jedno heslo ale je možné nastavit až pět možných hesel, která jsou potřeba znát pro přístup do poštovní databáze. Toto je možné využít například k superadminstrátorských účtům. Pro zalogování bude tak nutné více administrátorů, z nichž každý bude znát jedno heslo.
V běžných systémech je běžné, že administrátor je pánem všeho a má neomezený přístup ke všem datům. To je v Lotus Domino možno eliminovat. Lze systém nastavit tak, že administrátoři mají právo kompletně řídit a spravovat běh serveru, ale k vybraným citlivým databázím nebudou mít ani čtenářská práva, tím je možné znepřístupnit adminsitrátům například poštu VIP uživatelů. Všechny přístupy uživatelů k serveru se samozřejmě ukládají do logů, které lze dále prohledávat, zpracovávat a analyzovat dle libosti. Logy se zálohují po dobu, která je předem nastavena. Součástí Lotus Domino serveru jsou i nástroje, kterými se dají nastavit virtuální senzory, které hlídají výskyt určitých událostí v systému. V případě objevení takové události na ni zareagují například odesláním informativního e-mailu správci systému. Hlídanou událostí může být docházející místo na pevném disku, ale i neúspěšný pokus o přístup do libovolné databáze. [14]

3.3.6 Přístup k serverům a certifikáty

Přístup k serverům je v Lotus Notes zabezpečen tradičně pomocí souboru USER ID a také pomocí certifikátu. Certifikát neboli průkaz, je dokument prokazující nějakou skutečnost. Certifikát serveru zaručí, podobně jako razítko v pase, že jste osoba, za kterou se vydáváte. Při prvním přijetí ID souboru uživatele od administrátora systému obsahuje toto ID uživatele certifikát aplikaci Lotus Notes. Dále je možné využívat certifikáty sítě internet. Na certifikáty sítě internet se může odkazovat jako na certifikáty X.509. Všechny certifikáty se nahrávají do souboru uživatelského ID.

K přístupu na server Lotus Domino je nutné mít potřebný certifikát, který prokáže naši totožnost serveru, a server potřebuje certifikát, jímž naší totožnost ověří. Toto ověření tak funguje i opačně. Současné certifikáty aplikace Lotus Notes jsou hierarchické. To

znamená, že název certifikátčního úřadu tvoří součást názvu certifikátu, tedy našeho jména v systému. Certifikační úřad je entita, která vytvoří certifikát a vydá ho. Náš certifikát může vypadat například takto: Jakub Richtr/TEST, kde Jakub Richtr je naše jméno a TEST je název našeho certifikačního úřadu.

Typy certifikátů, které může ID obsahovat:

- **Víceúčelový certifikát programu Notes**: Tento certifikát slouží k identifikaci naší osoby pro většinu účelů aplikace Lotus Notes. Příkladem užití je například přihlášení do aplikace a přístup k Notes aplikacím na Lotus Domino serverech. Víceúčelové certifikáty aplikace Lotus Notes umožňují silné šifrování. Tento typ Notes certifikátu obsahuje soukromý a veřejný klíč. Tyto klíče slouží k podpisu a šifrování zpráv. Certifikát dále obsahuje název certifikačního úřadu, který ho vydal, dále pak jméno osoby nebo serveru, jemuž je certifikát vydán, datum vytvoření certifikátu a datum ukončení platnosti certifikátu.
- **Mezinárodní certifikáty programu Notes**: Mezinárodní certifikáty slouží pouze pro šifrování. Umožňují tak uživatelům, kteří nemohou používat silné šifrování, odeslat šifrovanou poštu. Tyto certifikáty nejsou obecně určené k osobnímu použití. USER ID obsahuje vždy jeden mezinárodní certifikát.
- **Běžné certifikáty**: Tyto certifikáty se užívaly v předchozích aplikacích Lotus Notes verze 4.6 a nižších a sloužily k přístupu do Lotus Domino serverů verze nižší než verze 5. Běžné certifikáty nemají hierarchické názvy a aplikace Lotus Notes od verze 5 již použití těchto certifikátů nepodporují.
- **Certifikát sítě internet:** Tento certifikát je třeba v případě přístupu k zabezpečenému webovému serveru, který vyžaduje připojení SSL. Při nastavení je třeba nastavit SSL port 433 a zvolit 128b šifrování RC4. Dále je tento certifikát potřeba pokud chceme šifrovat či podepsat poštu posílanou prostřednictvím sítě internet. Běžné úložiště certifikátů sítě internet je v prohlížečích sítě internet, jako jsou v Microsoft Internet Explorer, Mozilla FireFox, Gogole Chrome a další. Certifikáty sítě internet se ukládají i do ID souboru a je možné je tak užívat v aplikaci Lotus Notes. Certifikáty sítě internet často obsahují adresu elektronické pošty. Certifikát sítě internet může vypadat

například takto: CN=MMM Internet CA/O=MMM/S=BOSS/C=CZ. Část, kterou zobrazí aplikace Lotus Notes, je MMM Internet CA. Certifikáty sítě internet jsou Lotus Notes identifikovány jako víceúčelové certifikáty sítě internet. Tento typ certifikátu slouží v Lotus Notes k přístupu k zabezpečeným webovým stránkám prostřednictvím prohlížeče. Aplikace Lotus Notes pak odesílá a příjímá pošty pomocí S/MIME, které zajištuje zabezpečení. Certifikát slouží také k zabezpečenému připojení k službám stě internet pomocí připojení Secure Socket Layer. Certifikát sítě internet je možné použít jak k podpisu zprávy a jiný certifikát pak následně k jejímu zašifrování.

Obnovení certifikátu

ID soubor v sobě obsahuje víceúčelový certifikát programu Lotus Notes a dále také mezinárodní certifikát. Oba tyto certifikáty jsou platné po určitou dobu, základní nastavení je na 2 roky, poté je třeba před ukončením platnosti provést recertifikaci. Pokud certifikát neobnovíme před ukončením jeho platnosti, stane se neplatným a tím se stane neplatné i celé uživatelské ID. Jestliže neobnovíme víceúčelový certifikát programu k datu ukončení platnosti, budeme moci spustit aplikaci Lotus Notes, ale nebudeme se schopni přihlásit k Lotus Domino serveru. V takovém případě je třeba kontaktovat administrátora systému a provést recertifikaci svého ID. Při recertifikaci dochází pouze ke změně data ukončení jeho platnosti. Veřejné a soukromé klíče zůstávají beze změn. Pokud administrátor systému neobnoví certifikáty automaticky, obdržíme upozornění na datum ukončení platnosti certifikátu. V případě že má dojít ke změně certifikátu, systém uživatele na tuto eventualitu upozorní, ten pak musí recertifikaci akceptovat. [3, s. 225]

3.3.7 ID Vault

ID Vault je zabezpečené úložiště uživatelských ID souborů. Nelze ho však použít pro serverová a certifikační ID. Umožňuje automatickou synchronizaci více kopií ID souboru stejného uživatele a správu životního cyklu ID včetně změny jména a recertifikace. ID Vault zajišťuje snadnou obnovu ID v případě jeho ztráty či poškození. Je zde také možné resetování uživatelských hesel pověřenými osobami bez nutnosti administrátorských oprávnění.

Toto úložiště je součástí Lotus Domino od verze 8.5. ID soubory se do tohoto trezoru dostanou při registraci nového účtu. Je také možno nastavit synchronizaci ID či automatický upload přímo z klienta. Synchronizace je vhodná zejména k udržení aktuálních ID s aktuálními certifikáty v trezoru. Ke kontrole změn dochází každých 8 hodin.

Stažení ID souboru z trezoru je chráněn heslem. Tato databáze je šifrovaná pomocí ID serveru. Všechny ID soubory uložené v trezoru jsou zašifrované a nelze je tak při pouhém zkopírování použít. Hesla v ID mohou resetovat pouze administrátoři. Veškeré transakce mezi klientem a trezorem ID Vault jsou jak je v Lotus Notes samozřejmostí šifrované. [17]

4 Lotus Notes přes internet a mobilní telefon

4.1 LN přes internet

Lotus Notes nabízí standardně dvě možností přístupu k poště, kalendáři, úkolům a kontaktům přes webové rozhraní. První způsob, který je starší se jmenuje WebMail a použije se vždy, když je užita defaultní šablona pošty starších verzí Notes. To je například ve verzi Lotus Notes 6 šablona *mail6.ntf*. Tomu novějšímu se dříve říkalo iNotes, tento název byl později IBM změněn na Domino Web Access.

DWA je na úplně jiné úrovni, než WebMail, jak vzhledem, tak i funkčností a ovládáním. Pro jeho využití musíte poštovní databázi zaměnit návrhem ze šablony *iNotes6.ntf* a mít kompatibilní webový prohlížeč, což jsou vždy aktuální verze Internet Explorer a Mozilla Firefox. Pokud po připojení Domino detekuje nepodporovaný prohlížeč, zobrazí varování a nabídne použití jednoduššího rozhraní WebMailu. V případě, že je webový prohlížeč pořádku je třeba povolit, stáhnout a nainstalovat potřebné certifikáty.

Od verze Domina 6.5.4 lze použít rozhraní, které se jmenuje Domino Web Access - Lightweight UI, neboli zkráceně iNotes Lite. Poštovní šablona iNotes6.nsf v sobě obsahuje všechny tři rozhraní a umožňuje mezi nimi přepínat. Přepínání je možné buď ručně, nebo automaticky podle detekovaného browseru. Pokud tedy víme, že náš prohlížeč má na víc, než na zastaralý WebMail, je možné přepnout UI na iNotes Lite.

iNotes Lite od plnohodnotného iNotes liší zejména odstraněním několika nepodstatných prvků pro jeho provoz. Z návrhu byla odstraněna spousta zkrášlujících prvků, jako oblé rohy záložek, zjednodušily se posuvníky, na pozadí není gradient, ale je jednobarevné. Nastavit iNotes Lite hromadně pro všechny uživatele na serveru lze provést změnou parametru v notes.ini na: *iNotes_WA_UI=inotes_lite*. [12]

4.2 LN přes mobilní telefon

4.2.1 OneBridge

OneBridge Mobile Groupware je software pro mobilní přístup z mobilních zařízení k e-mailům, kalendáři, úkolům, poznámkám nebo databázím. OneBridge tak umožňuje uživatelům v terénu stálý přístup do své poštovní schránky a průběžnou synchronizaci důležitých dat. OneBridge podporuje jak Lotus Domino, tak i například MS Exchange. Poštu je možné synchronizovat téměř se všemi mobilními zařízeními, které pro to mají vhodný software. Jedná se tak v současnosti o všechny nové typy mobilních telefonů, což je velkou předností softwaru OneBridge.

Tento mobilní software je vhodný pro firmy, které chtějí připojit své uživatele pomocí mobilních telefonů nebo PDA zařízení do podnikových systémů Lotus Domino či MS Exchange. OneBridge podporuje například mobilní zařízení, jako jsou Nokia 9300, Sony-Ericsson P910, Smartphone, Palm Treo, MDA a další. Jeho další výhodou je jeho cena, která je oproti konkurenci díky svému volnému obchodnímu modelu výrazně zajímavější.

OneBridge synchronizuje e-maily a všechny změny na poštovním serveru s mobilním zařízením a naopak automaticky bez nutnosti jakékoli aktivity ze strany uživatele. To samozřejmě za předpokladu vhodné konfigurace. Uživatel tak má ve svém mobilním zařízení k e-mailům, kalendáři, kontaktům, úkolům nebo poznámkám ze svého poštovního klienta snadný a okamžitý přístup. OneBridge umožňuje mimo automatické synchronizace také ručně vyvolanou synchronizaci přímo uživatelem. Ta se osvědčí zejména v zahraničí při roamingovém připojení, kdy si uživatel sám může regulovat limit stažených dat.

Jak již bylo zmíněno OneBridge podporuje velkou řadu mobilních zařízení. Poštovní klienti jsou kompatibilní s operačními systémy jako je Palm OS, Symbian, PocketPC, Windows Mobile a SyncML. Dále je také možný přístup do pošty přes WAP, který je dostupný v současné době v každém mobilním telefonu.

Ovládání celého softwaru je velmi jednoduché. Stačí k němu pouze jedno tlačítko mobilního telefonu. Uživatelé tak nemusí dělat žádné nastavení navíc k tomu, aby se dostali z mobilního telefonu do své firemní pošty tak podporuje jak messaging, tak i synchronizaci různých firemních databází v Lotus Notes.

Díky dobrému administrátorskému rozhraní má každý administrátor OneBridge přehledný a snadno ovládaný nástroj pro rychlou a efektivní administraci všech mobilních zařízení a uživatelů z jednoho prostředí.

Minimální požadavky na server:

- Pentium III 500 MHz
- 256 MB RAM
- 100 MB volného místa na disku
- 4 MB místa na disku pro každého uživatele
- TCP/IP LAN připojení

Podpora OS:

- Palm OS 3.5.1 +
- WinCE
- Symbian 6+
- SyncML
- Windows Mobile 2002+

V současné době však již využití OneBridge není příliš aktuální jelikož společnost Sybase ukončila 31.8.2010 jeho podporu. [19]

4.2.2 BlackBerry

BlackBerry je kombinace služeb a hardware vyvinutá firmou Research in Motion, která umožňuje neustálou synchronizaci dat mezi mobilním zařízením a firemním serverem. BlackBerry Enterprise Server je serverový software zajišťující komunikaci a synchronizaci se zařízeními BlackBerry či jinými mobilními zařízeními, které podporuje. BES podporuje dále například telefony Nokia, iPhone, nebo telefony s operačním systémem Android.

BlackBerry tak svým uživatelům nabízí možnost pracovat s firemní poštou včetně příloh, synchronizovat schůzky na firemním serveru nebo přistupovat k databázím či aplikacím na serveru.

5. listopadu 2010 společnost Research In Motion vydala novou verzi softwaru BlackBerry Enterprise Server Express, která podporuje servery běžící na IBM Lotus Domino. To znamená, že pokud společnost využívá Lotus email, může zdarma používat BES Express a pomocí něho synchronizovat emaily, kalendář, kontakty, poznámky a úkoly mezi zařízeními BlackBerry a serverem IBM Lotus Domino bez nutnosti řešit další bezpečnostní problémy. Díky BlackBerry Enterprise Server je možné bezdrátově synchronizovat emaily, kalendář, kontakty, úkoly a poznámky, dálkově spravovat emailové složky a hledat emaily na serveru. Dále pak také snadno spravovat schůzky, jednání a organizovat čas. V případě, že má například uživatel dovolenou může nastavit automatickou odpověď „mimo kancelář“, čímž zajistí informaci pro všechny uživatele, kteří mu v té době pošlou poštu, informaci o jeho nedostupnosti. Díky BES je možné přistupovat k datům a souborům na firemní síti a využívat mobilní aplikace k přístupu k podnikovým systémům za firewallem. Administrátoři navíc můžou pomocí webového rozhraní dálkově snadno spravovat a přidávat zařízení BlackBerry, nahrávat a spravovat aplikace v zařízení nebo aplikovat IT zásady použití. BlackBerry Enterprise Server Expres pracuje s Domino Enterprise Serverem a s Domino Messaging Serverem.

Zabezpečení BlackBerry Enterprise Serveru je navrženo tak, aby vyhovělo těm nejpřísnějším požadavkům na ochranu a zabezpečení citlivých dat. Data jsou tak na mobilním zařízení pouze v šifrované podobě, s možností jejich centrální správy.

V případě ztráty nebo odcizení lze zařízení ihned dálkově odpojit od firemní sítě a zabránit tak úniku citlivých dat, případně je možné speciálním softwarem veškerá data z paměti telefonu na dálku vymazat. Pomocí šifrování 3DES a AES je zajištěna vysoká ochrana dat přenášených mezi serverem a BlackBerry zařízením. BES nabízí také podporu politiky rozdílných přístupových práv pro jednotlivce a skupiny uživatelů. [7]

4.2.3 Lotus Notes Traveler

IBM Lotus Notes Traveler je sada produktů, která umožňuje synchronizaci dat mezi Lotus Notes a mobilním zařízením. Tato synchronizace tak probíhá nejčastěji přes GPRS/EDGE nebo WiFi. Pomocí Traveleru lze stejně jako u předchozích řešení synchronizovat poštu, kalendář, kontakty a poznámky. Data se na straně klienta ukládají do mobilního zařízení. V něm jsou pro data vytvořeny příslušné programy a to poštovní klient, kalendář a správce kontaktů. Traveler pro čtení pošty využívá pragramy mobilního zařízení, jelikož sám o sobě tyto programy neobsahuje.

Traveler se skládá z:

- **Traveler klient** – klient se instaluje na mobilní zařízení a stará se o spojení a synchronizaci se serverem
- **Traveler server** – se instaluje na Lotus Domino server. Traveler se skrze něj dostává k datům v poštovní databázi. Data následně přenáší do mobilního zařízení.

Společnost Nokia, která u svých vybraných modelů oficiálně podporuje Lotus Notes Traveler poskytuje možnosti vyššího zabezpečení dat Lotus Notes Traveleru od verze 8.5.1. Ve starších verzích nebyla tato nastavení dostupná. Jedná se zejména o

konfiguraci zařízení dle Domino serveru, zakázání synchronizace, nastavení síly hesla, nebo možnosti smazání dat z mobilního zařízení administrátorem na dálku.

Pro aplikaci vyššího zabezpečení pro Traveler je třeba z oficiálních stránek společnosti Nokia stáhnout instalační soubor Lotus Traveler Security enablement. Tento software je pak nutné nainstalovat do mobilního telefonu stejně jako ostatní aplikace. Po spuštění Traveleru na mobilním telefonu si můžeme projít jednotlivé možnosti, které jsme instalací získali, a které nám politikou Domino serveru byly nakonfigurovány do nastavení, se dostaneme v mobilním telefonu přes možnost *Traveler – Tools – View security*. [9, 13]

Od verze Lotus Domino 8.5.2 přichází nový Lotus Traveler s významnými novinkami. Těmi jsou rozšířená podpora serveru pro operační systém Linux. Ten je možné instalovat i na operační systémy SUSE Linux Enterprise 10.2 32-bit a 64-bit, SUSE Linux Enterprise 11 32-bit a 64-bit a Red Hat Enterprise Linux 5 32-bit a 64-bit.

Dalším přínosem této verze je možnost uživatelsky spravovat zabezpečení Traveleru. Uživatelé mohou sami vzdáleně vymazat, nebo zamknout své vlastní zařízení, bez pomoci administrátora.

Komunikace mezi Lotus Notes Traveler serverem a zařízením je možné realizovat přes HTTP nebo HTTPS. Lotus Notes Traveler klient se systémem Windows Mobile nebo Symbian již nepoužívá samostatné TCP spojení přes port 8642 pro zprávy. Lotus Notes Traveler server však i nadále podporuje starší klienty, které stále tento port používají. Pokud však všichni uživatelé mají klienta 8.5.2, není nutné port TCP v nastavení serveru povolovat. [20]

5 Bezpečnost Lotus Notes

Předmětem vlastní práce je navrhnout řešení v Lotus Notes dle předem daného zadání. Důraz je kladen zejména na možnosti nastavení zabezpečení. Tato práce se tak pokusí demonstrovat možnosti využití Lotus Notes.

5.1 Zadání

Zadání pro realizaci bylo sestaveno na základě konzultace s vedoucím pracoviště servisu. Jedná se tak o reálný přehled požadavků na poštovní systém pro pracoviště servisu. Seznam je však neúplný a obsahuje jen základní body pro demonstraci využití programu Lotus Notes.

Požadavky:

- Vytvořit uživatelský účet
- Kapacita schránky minimálně 300MB
- Možnost archivace
- Zabezpečený přístup ke všem datům na disku
- Elektronický podpis
- Možnost sdílení mailů mezi uživateli
- Přístup k poště i z mimopodnikové sítě
- Možnost okamžité blokace uživatele
- Zástupná schránka pro pracovníky servisu – ve stejné směně bude s jednotlivými maily/úkoly pracovat více pracovníků naráz
- Z bezpečnostních důvodů pracovníci servisu nemají možnost mazat e-maili, o celou správu schránky se bude starat jeden manager, který může případně delegovat práva na jiného uživatele
- Možnost přístupu do pošty přes web
- Možnost přístupu do pošty přes mobilní telefon

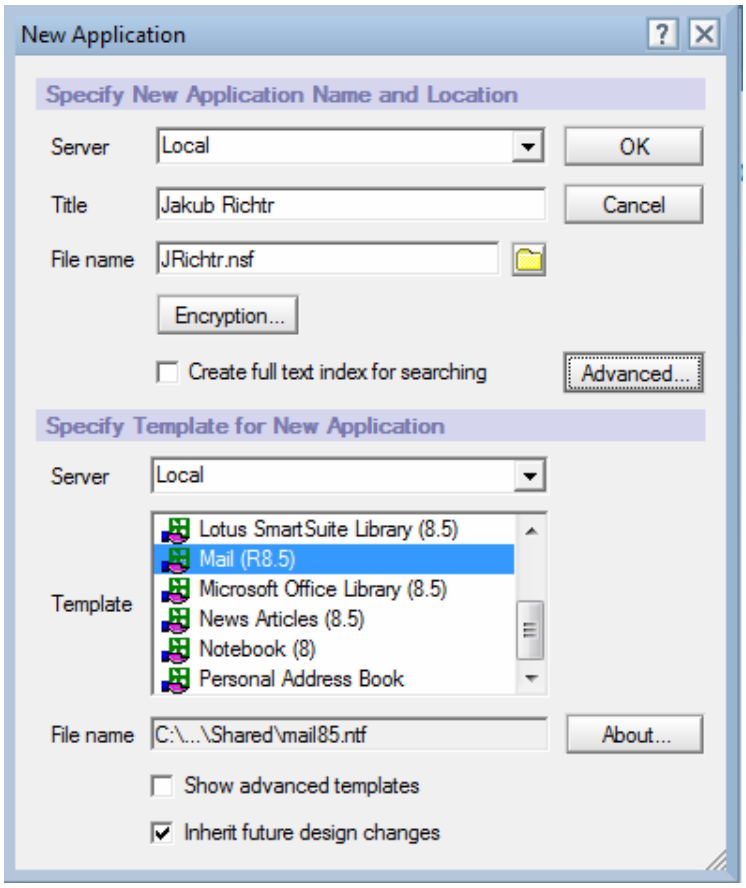
5.2 Návrh řešení

5.2.1 Tvorba a nastavení uživatelského účtu

Prvním krokem je vygenerování uživatelského ID, do kterého jsou nahrány potřebné certifikáty a nastaveno výchozí heslo pro instalaci. ID je po vygenerování umístěno na server, kde čeká do první instalace klienta.

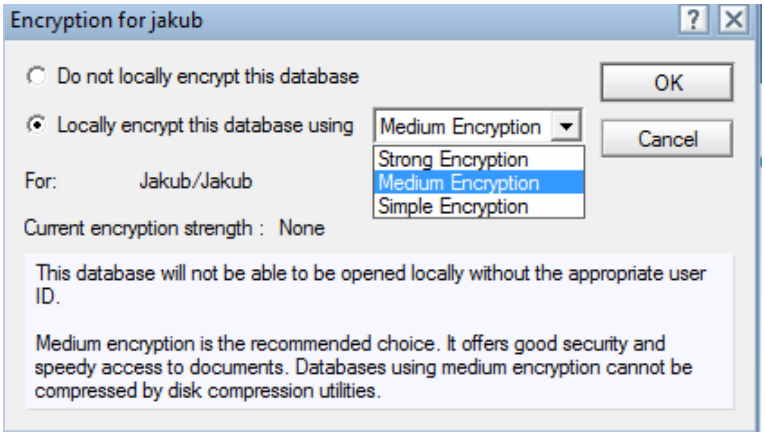
Dalším krokem je vytvoření poštovní databáze na příslušném serveru. Poštovní databáze se vytváří obdobně jako jakákoli jiná databáze na serveru *File-Application-*

New. Při tvorbě vybereme server, kde bude databáze umístěna. Poté nastavíme šablonu pro databázi. Vybereme server, na kterém jsou připravené šablony, a vybereme vhodnou. Pro náš případ poštovní databáze zvolíme Mail (R8.5), což je šablona verze 8.5 poštovní databáze, jak pro klienta, tak pro webový přístup. Je možné si vytvořit i vlastní šablonu nebo upravit předem připravené.



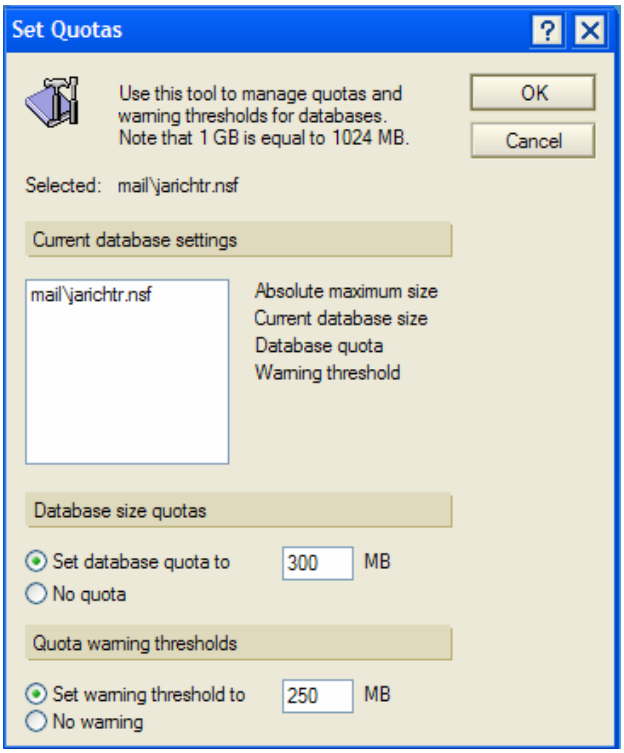
Obrázek 5.1 - Vytvoření nové databáze

V případě, že bude umístěna na lokální disk, je vhodné nastavit šifrování. Na výběr máme tři druhy šifrování a to Strong, Medium a Simple. Při výběru šifrování je třeba zvážit, jak moc je důležité mít databázi šifrovanou. Síla šifrování ovlivňuje následně i dobu otevírání databáze, proto je třeba rozhodnout, co bude pro uživatele v dané situaci nejvhodnější. Pro náš případ zvolíme Medium Encryption.



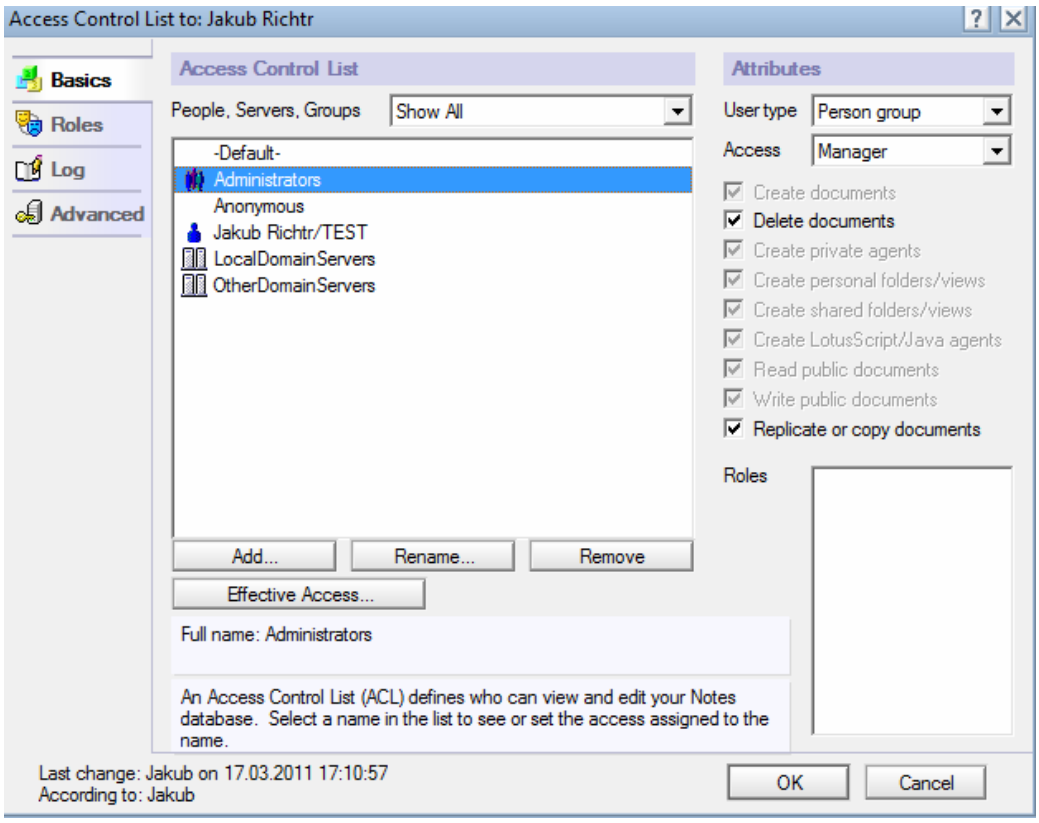
Obrázek 5.2 - Nastavení šifrování

Následně spustíme Lotus Administrator a na příslušném serveru najdeme vytvořenou databázi. V záložce Configuration zvolíme Set Quotas a nastavíme povolenou kapacitu poštovní schránky a práh varování. Při dosažení prahu varování bude uživatel při spuštění klienta upozorněn. V případě, že dosáhne či překročí nastavenou quotu přestanou se mu ukládat odeslané emaily. Pošta mu i přesto bude stále chodit.



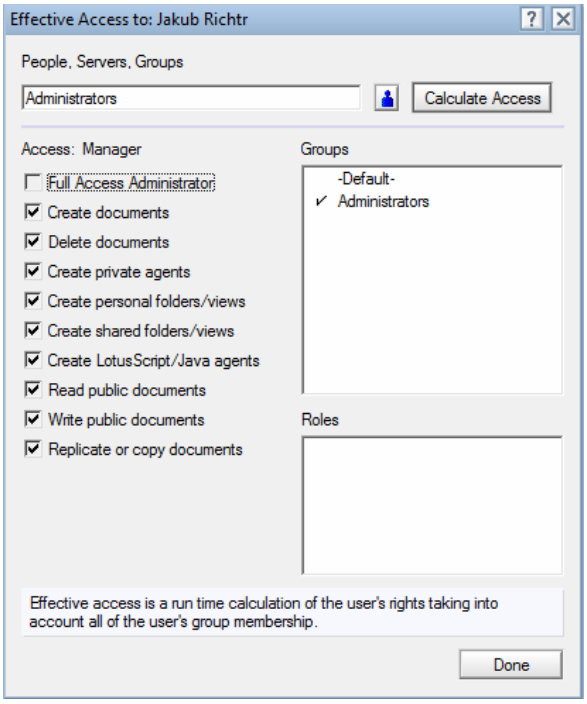
Obrázek 5.3 - Nastavení quoty mailboxu

Po vytvoření databáze je třeba nastavit její Access Control List *(File-Application-Access Control)*, v kterém je možné nastavit veškerá přístupová práva v poštovní databázi. Práva můžeme přidělovat osobám, nebo skupinám osob. Do ACL přidáme skupinu Administrators zvolíme typ Person group a Access Manager standardní přístupová práva této skupiny doplníme ještě o možnost Delete documents.



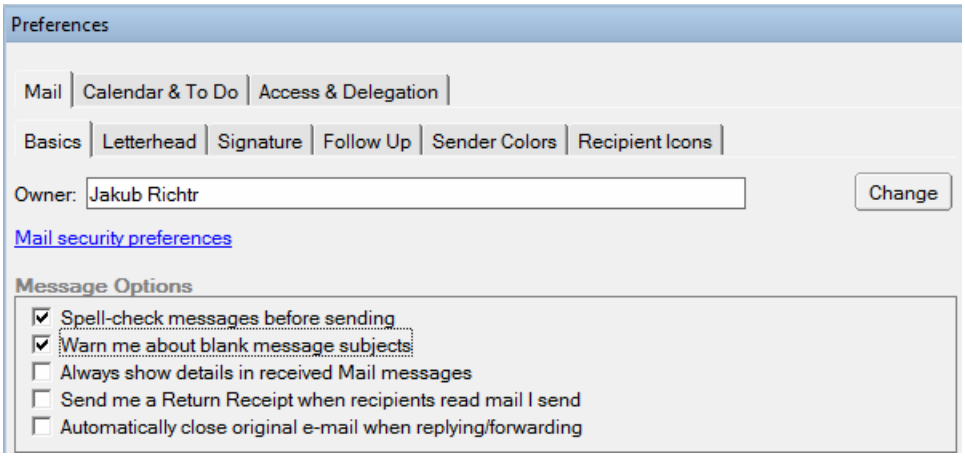
Obrázek 5.4 - Nastavení ACL

Následně ještě v Effective Access nastavíme Full Access Administaror. Díky této skupině budou moci administrátoři systému spravovat tuto poštovní databázi. Bezpečnost je zajištěna logy, do kterých se ukládají veškeré změny a činnosti jednotlivých uživatelů/skupin v této databázi.



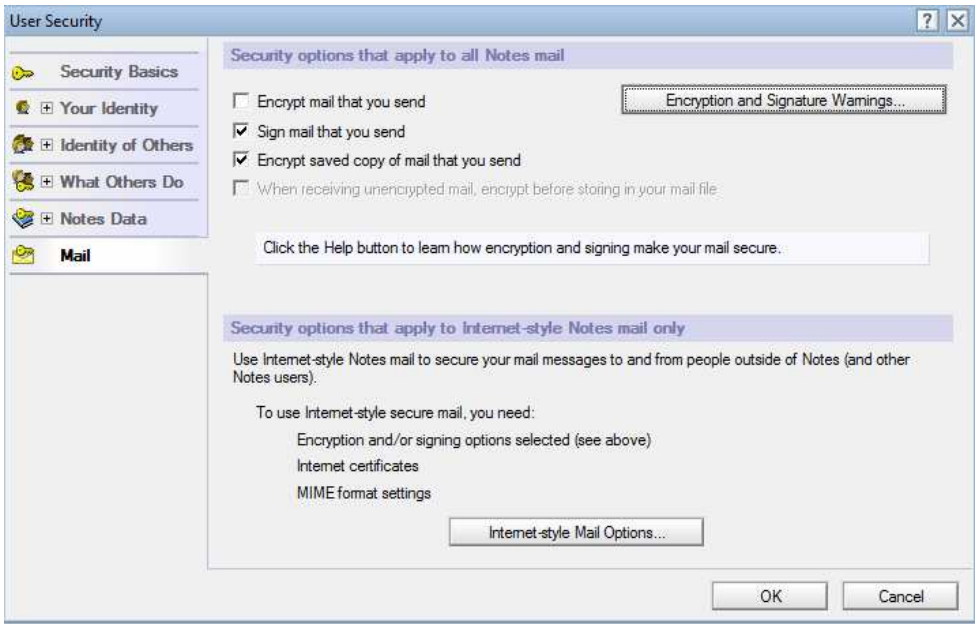
Obrázek 5.5 - Nastavení ECL

Po nastavení přístupových práv je nutné nastavit vlastníka vytvořené databáze, v otevřené poštovní databázi tedy zvolíme možnost Preferences a v záložce Basic zvolíme vlastníka (Owner). Poté ještě nastavíme vlastnosti, které usnadní uživateli práci, jako jsou kontrola pravopisu před odesláním a varování před odesláním.



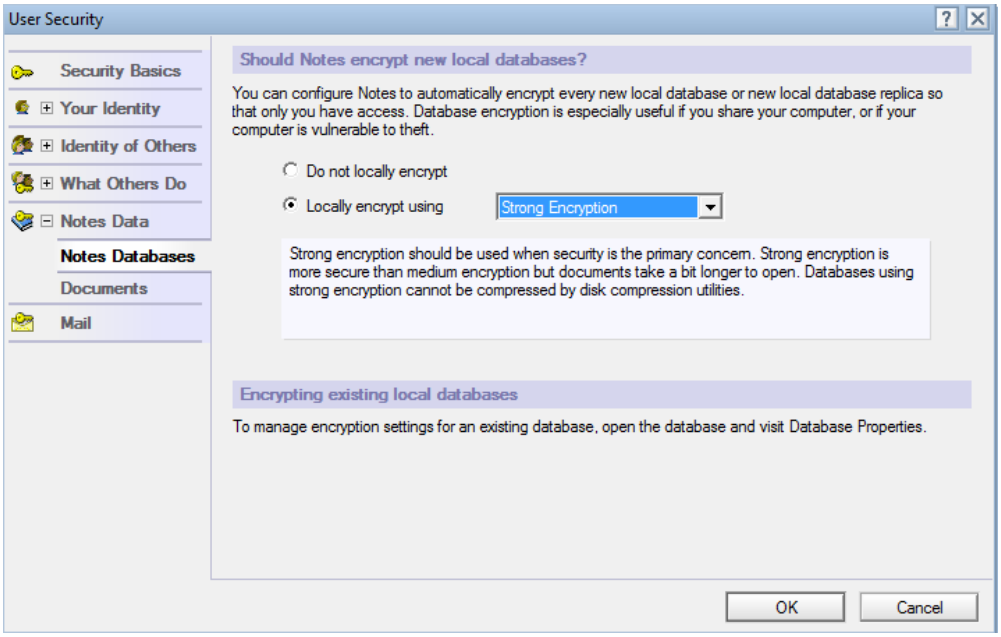
Obrázek 5.6 - Zadání vlastníka v předvolbách

V Preferences dále zvolíme možnost Mail Security preferences pro nastavení dalšího zabezpečení. Zde v záložce Mail nastavíme elektronický podpis odchozích zpráv uživatelem a šifrování uložených odeslaných zpráv.



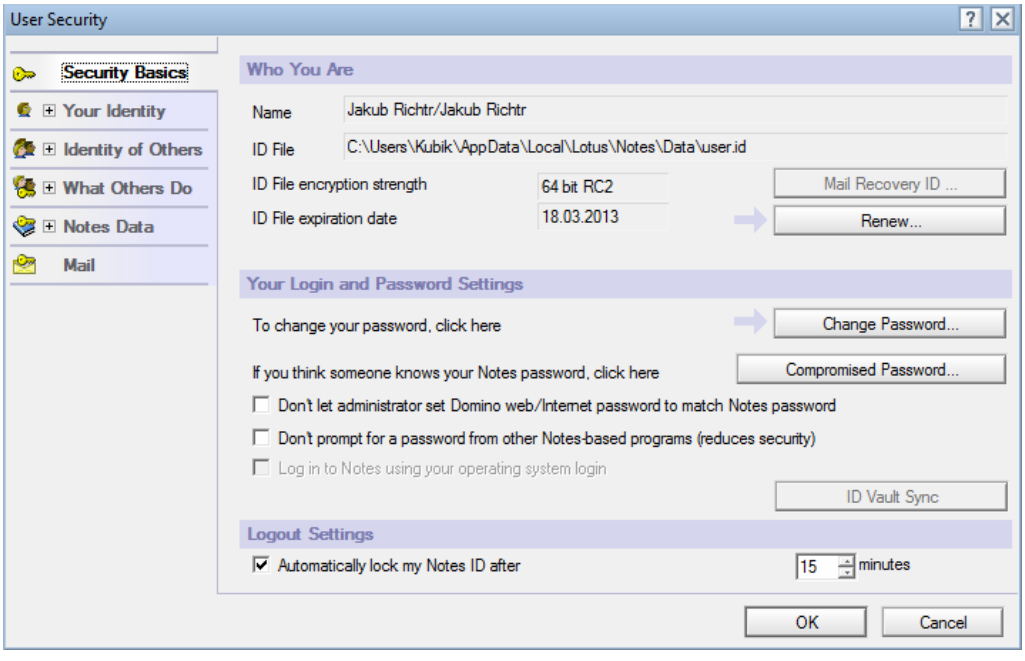
Obrázek 5.7 - Uživatelské předvolby - automatický podpis

Pro nastavení zabezpečení dat v databázích přejdeme do záložky Notes Data, kde dle uživatelských požadavků nastavíme Strong encryption pro vysoké zabezpečení dat na lokálním disku, tím docílíme toho, že databáze bude moci otevřít pouze uživatel, který je svým klíčem zašifroval.



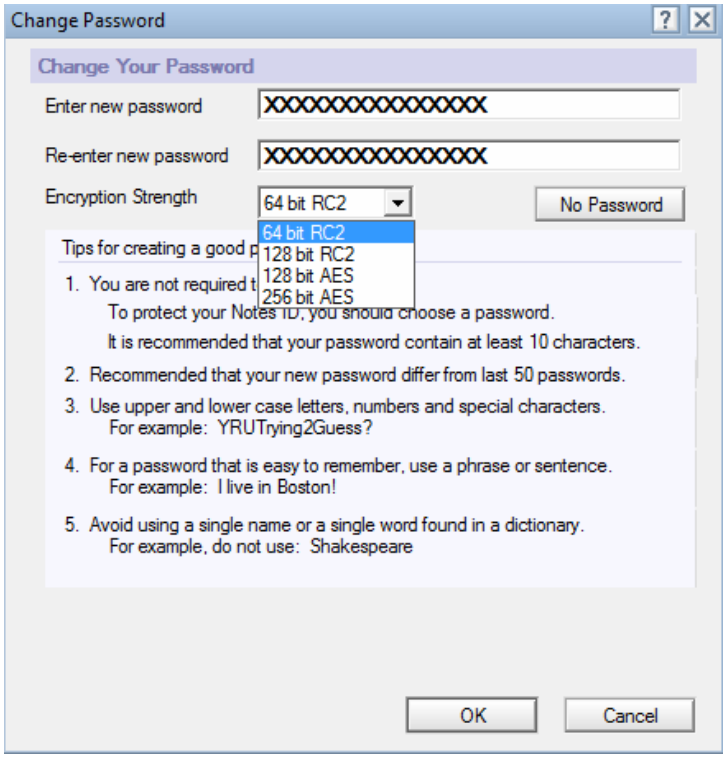
Obrázek 5.8 - Uživatelské předvolby - šifrování

V záložce Security Basics můžeme zkontrolovat platnost certifikátu ID souboru. Při jeho expiraci je nutná recertifikace. Dobu platnosti certifikátu je možno libovolně nastavit. Běžně se používají dva roky. Z důvodů větší bezpečnosti nastavíme možnost automatického zamykání klienta při nečinnosti na 15 minut. Uživatel musí poté pro odemknutí znovu zadat heslo.



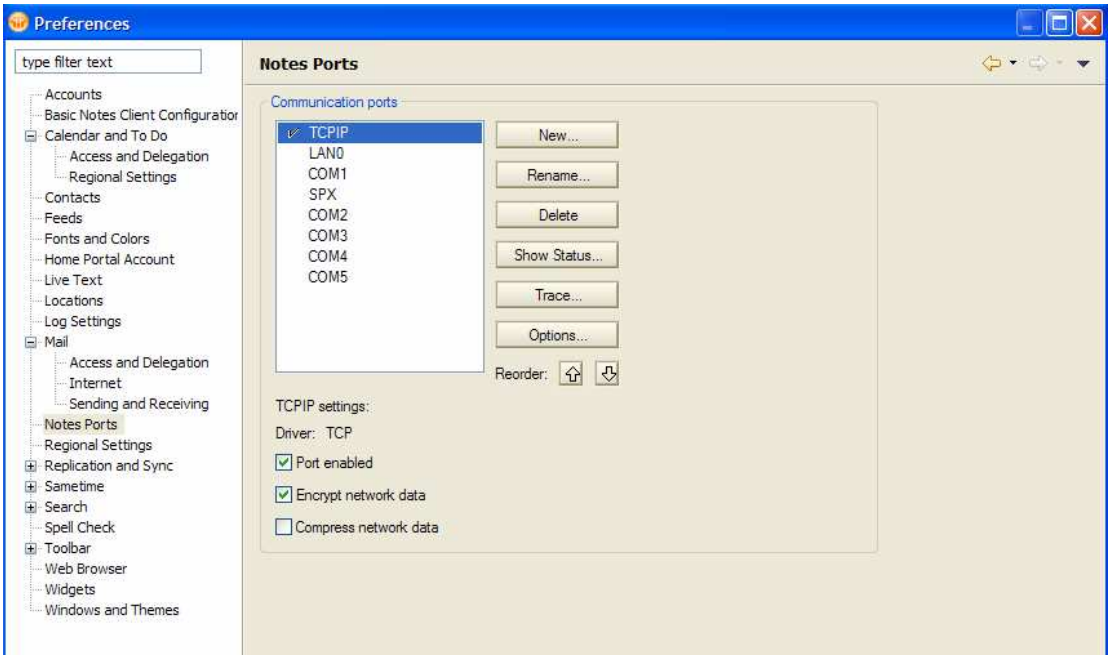
Obrázek 5.9 - Automatické zamykání klienta

Dále zde nalezneme tlačítko pro změnu hesla. Při změně hesla je možné nastavit i sílu šifrování pro naše účely zvolíme 64bit RC2. Novou funkcí v Lotus Notes od verze 8 je ID Vault, díky kterému je ID uživatele synchronizováno v zabezpečeném trezoru na serveru a po případné ztrátě ID je možná jeho obnova či při zapomenutí hesla je jednodušší obnova hesla.



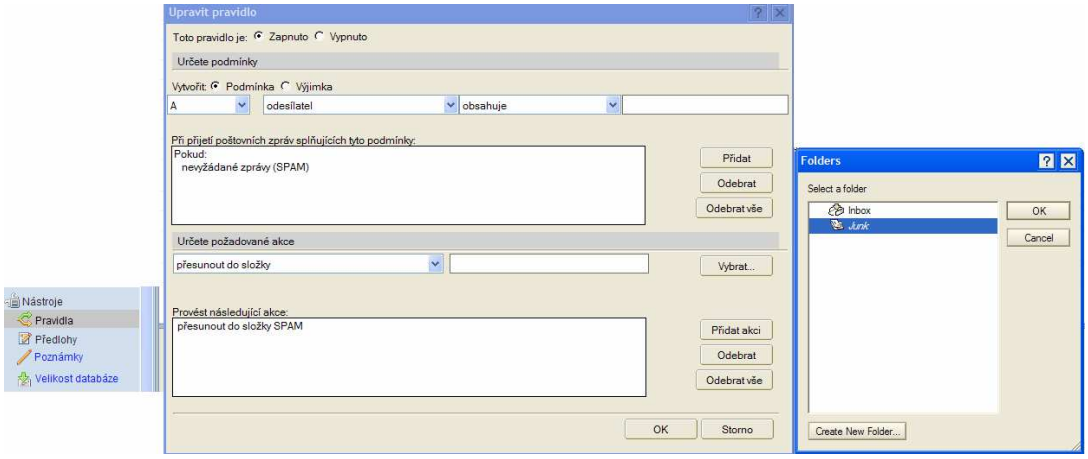
Obrázek 5.10 - Volba síly šifrování hesla ID

Vzhledem k tomu, že uživatelé budou přistupovat k serverům i z vnější nezabezpečené sítě je nutné nastavit šifrování přenosu. To provedeme *v File-Preferences-Notes Ports*, kde nastavíme šifrování u portu TCP/IP. Pro nastavení vybereme Encypt network data.



Obrázek 5.11 – Šifrování u portu TCP/IP

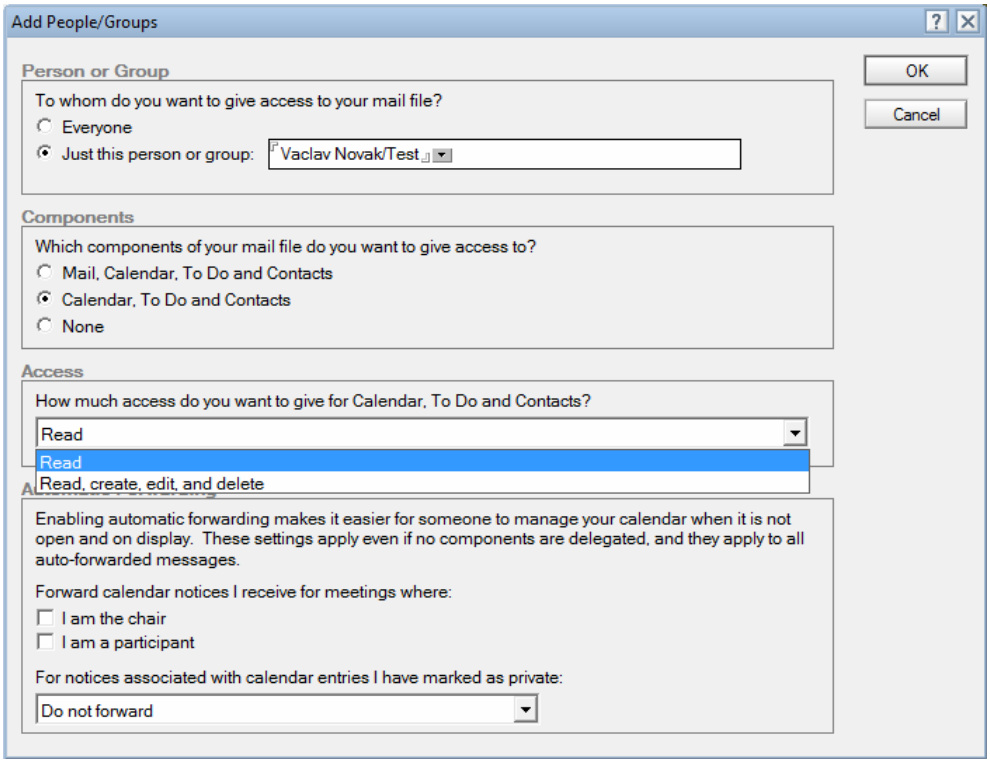
K odfiltrování nevyžádané pošty, kterou přímo nezachytí spamfiltr použijeme možnost vytváření pravidel. Pravidlo vytvoříme přes *Tools-Rules-New*. V intuitivním editoru následně nastavíme pravidlo, které bude obsahovat podmínku - pokud odesílatel obsahuje nevyžádané zprávy – přesunout do složky Junk mail. Po stisknutí klávesy OK se pravidlo automaticky spustí na serveru. Pokud chceme pravidlo smazat, je nutné ho nejprve deaktivovat. V případě, že uživatel smaže aktivní pravidlo ze seznamu to mu sice zmizí, ale na serveru bude stále aktivní a uživatel k němu již nebude mít přístup a bez pomoci administrátora ho již nedeaktivuje. Toto je jeden z nedostatků Lotus Notes, který se objevuje již v několikáté verzi.



Obrázek 5.12 - Tvorba pravidla

5.2.2 Delegování práv

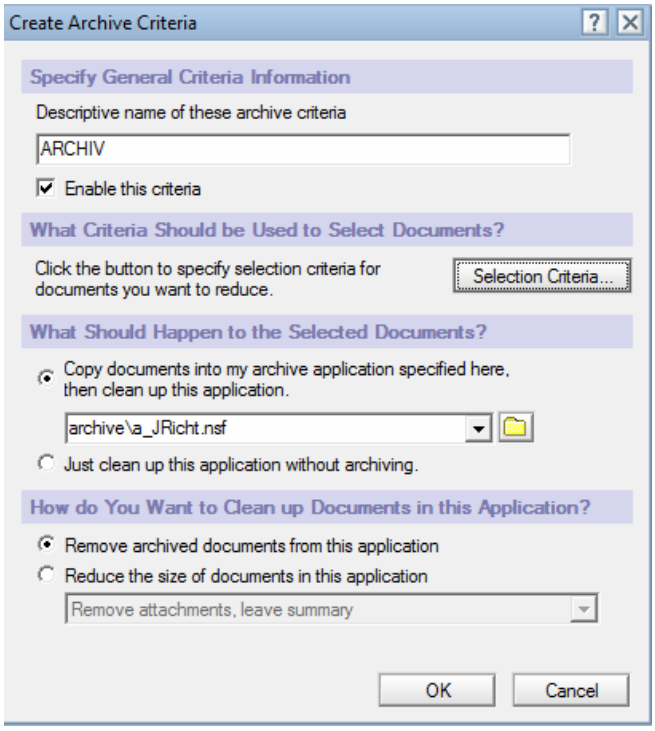
Po nastavení pravidel přejdeme k uživatelskému rozhraní delegování a přidělování přístupových práv a to k poště, úkolům, kalendáři či osobním kontaktům. Na výběr jsou dvě skupiny práv a to práva ke čtení a druhá skupina obsahuje práva ke čtení, vytváření, editaci a mazání. Podrobnější nastavení přístupových práv lze provést pouze v ACL. Toto nastavení nalezneme v *File-Preferences-Access and Delegation*. Dle požadavků přidělíme přístupová práva uživateli do kalendáře, úkolů a osobních kontaktů. A vybereme skupinu práv pouze ke čtení. Vybraný uživatel tedy bude moci prohlížet kalendář, úkoly a kontakty. Práva můžeme přidělovat jak jednotlivým uživatelům, tak skupinám.



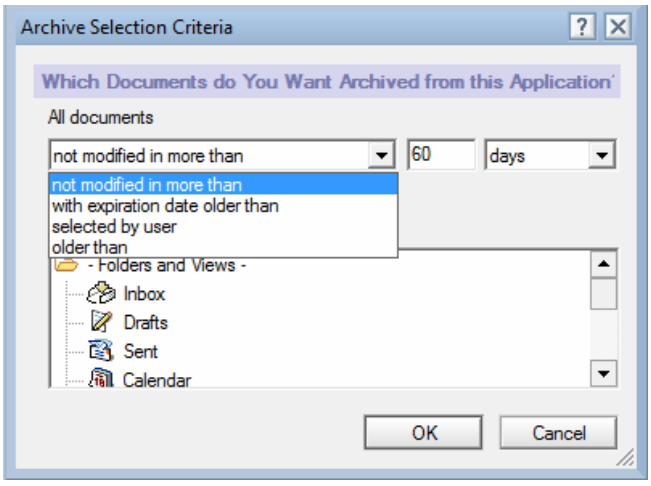
Obrázek 5.13 - Delegování práv

5.2.3 Nastavení archivace

Vhledem k omezené kapacitě poštovní schránky na serveru pro každého uživatele je nutností nastavit v Lotus Notes archivaci. Ta zajistí přesunutí dat ze serveru na lokální disk. Pro nastavení archivace zvolíme *Actions-Archive-Settings*. Zde zadáme jméno archivu a cestu k němu. Dále nastavíme kritéria archivace. Vybrat si můžeme z několika variant. Pro naši potřebu zvolíme kriteria, která zajistí přesun mailů, které nebyly otevřeny déle jak 60dní. Posledním krokem je nastavení času automatické archivace v záložce Schedule. Po nastavení archivace je nutné archivaci spustit a tím aktivovat veškerá nastavená kriteria. To provedeme příkazem *Actions-Archive-Archive Now*.



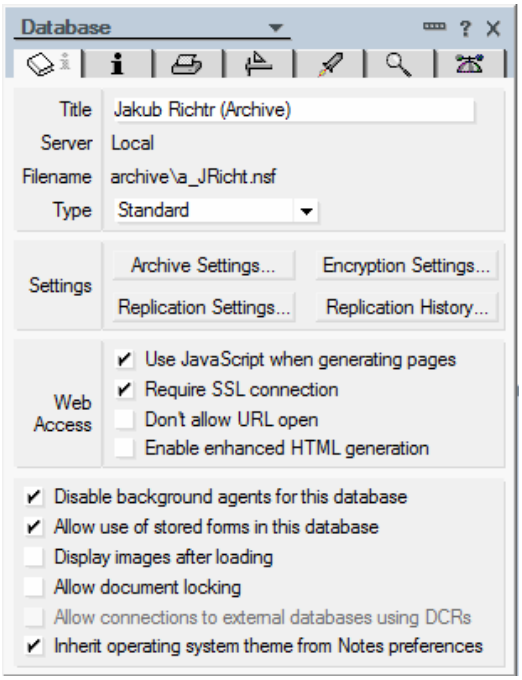
Obrázek 5.14 - Tvorba archivu



Obrázek 5.15 - Nastavení kriterií archivace

Jelikož se archivované emaily ukládají na lokální disk, je třeba nastavit šifrování. To nám zajistí, že přístup do archivu bude mít pouze jeho vlastník, který ho svým ID zašifroval. Po otevření archivu zvolíme *File-Application-Properities*. V tabulce následně nastavíme SSL connection, které zajistí zabezpečenou komunikaci mezi serverem a klientem při přístupu do databáze přes webový prohlížeč. V Encryption

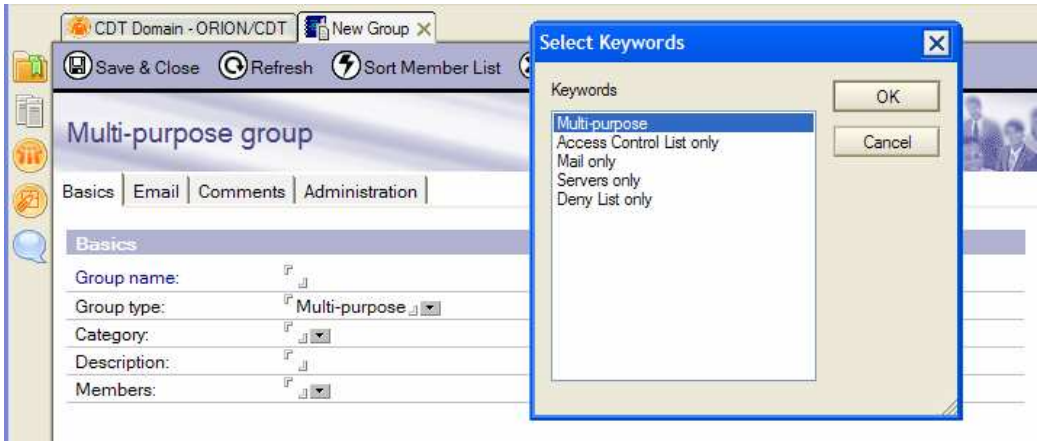
Settings nastavíme Medium Encryption, které zajistí šifrování databáze archivu na lokálním disku.



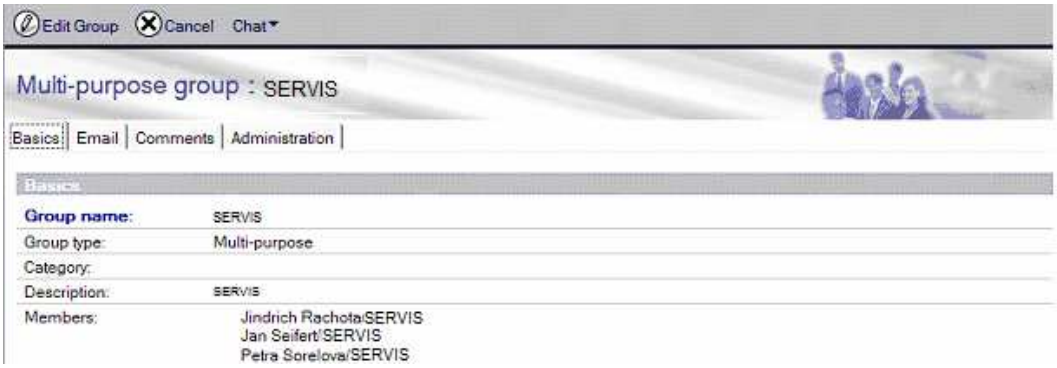
Obrázek 5.16 - Šifrování archivu

5.2.4 Tvorba skupin

Pro jednodušší práci s přidělováním práv a možnosti hromadného odesílání mailů celé skupině, vytvoříme skupinu s těmito vlastnostmi pro pracovníky servisu. Otevřeme Adresní seznam a vybereme záložku Groups, v které zvolíme možnost New Group. Při tvorbě skupiny je nutné zadat název a nastavit typ, který je možné vybrat z pěti předem daných. Zvolíme typ Multi-purpose, který zajistí, že bude možno skupinu užívat jak ACL, tak také jako distribuční seznam. Jelikož bude skupina sloužit jako distribuční seznam, je nutné nastavit v záložce email její smtp adresu. V případě, že bude mail adresován na tuto skupinu, dojde všem jejím členům. Posledním krokem je přidání členů do skupiny.



Obrázek 5.17 - Vytvoření skupiny



Obrázek 5.18 - Nastavení skupiny

5.2.5 Blokování uživatele

K zajištění okamžitého blokování účtu vytvoříme skupinu s typem Deny List. Uživatelé, které do ní vložíme tak budou mít zablokovaný přístup na poštovní server. Při přihlašování projdou pouze přes autentizaci, ale při testu autorizace jim již server oznámí nedostatečná přístupová práva k databázi na serveru a dál je nepustí. Do skupiny je možné uživatele přidávat či mazat manuálně, nebo lze nastavit agenta, který tento úkon bude provádět automaticky. A to například na základě informací z databáze personalistiky.

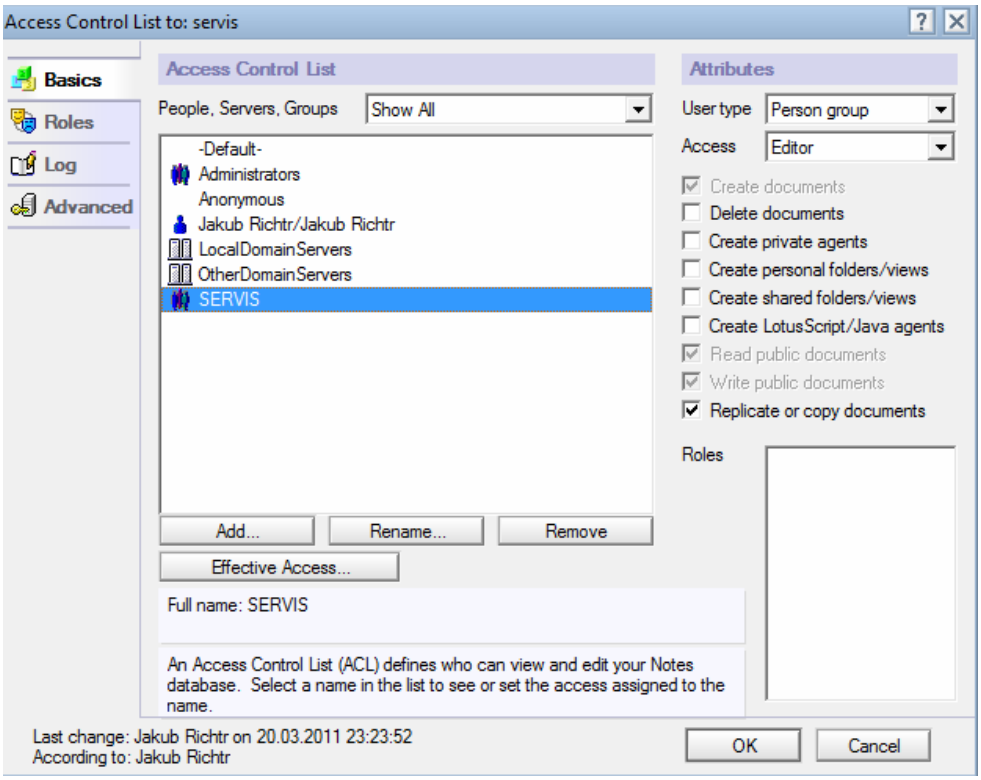
Obrázek 5.19 - Skupina pro blokování uživatelů

5.2.6 Tvorba a nastavení zástupné schránky

Zástupnou schránku vytvoříme stejným způsobem jako schránku uživatelskou. Jediný krok, který odpadne, bude vytvoření ID souboru. Tato schránka tak tedy nebude přístupna pod heslem a ID ale budou do ní mít přístup uživatelé, kteří své ID vlastní a mají příslušná práva v ACL této zástupné schránky. Aby zástupná schránka plnila svůj účel, což je možnost všech členů pracovat s příchozí poštou. Schránka proto musí mít vlastnost, která zajistí okamžité označení mailu, s kterým již někdo pracoval (otevřel ho). To nám zajistí speciální šablona, která tuto funkci obsahuje. Při tvorbě databáze tedy musíme příslušnou šablonu nastavit.

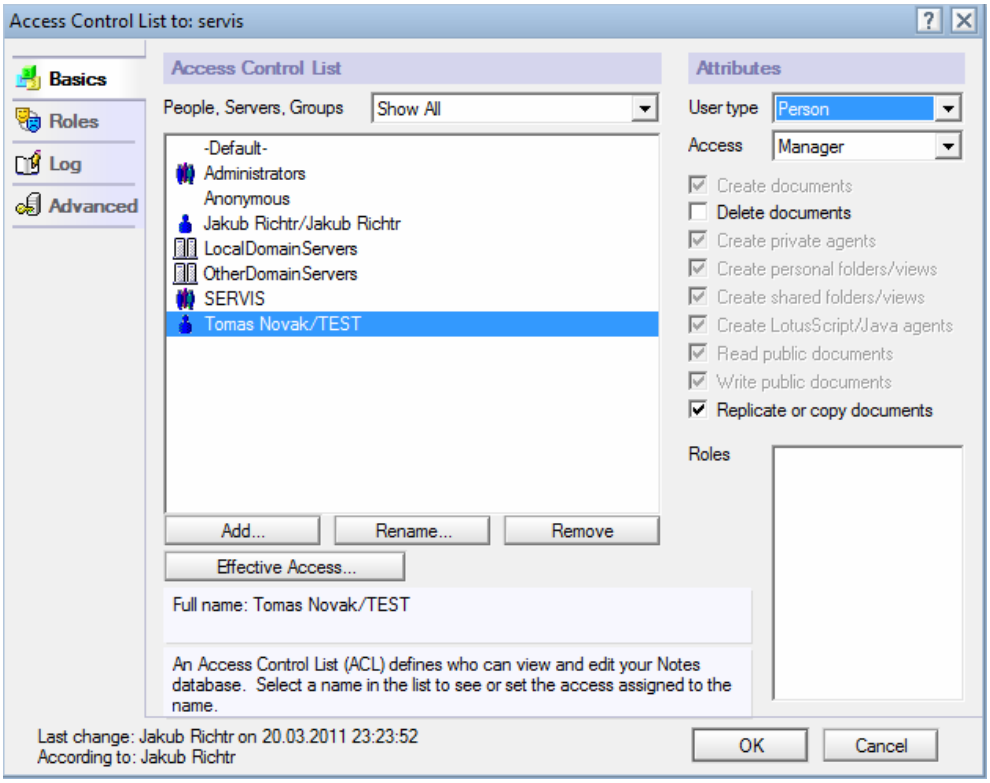
Obrázek 5.20 - Náhled zástupné schránky

Ve vytvořené zástupné schránce dále nastavíme přes *File-Application-Access Control* přístupová práva. Přidáme pro tento účel vytvořenou skupinu SERVIS, této skupině nastavíme přístupová práva typu Editor. Tato skupina práv zajistí potřebnou práci (vytváření a čtení) mailů. Uživatelé této skupiny nebudou mít možnost došlou poštu mazat.



Obrázek 5.21 – Přidání skupiny do ACL

Následně přidáme managera schránky, který bude mít možnost přidávat další uživatele a editovat jejich oprávnění. Přidáme mu ještě možnost Delete documents, aby mohl mazat potřebné zprávy. Do schránky samozřejmě ještě musíme přidat skupinu Administrators, která zajistí veškerou administrátorskou správu této schránky. A dále nastavíme v Lotus Administrátoru kapacitní omezení.

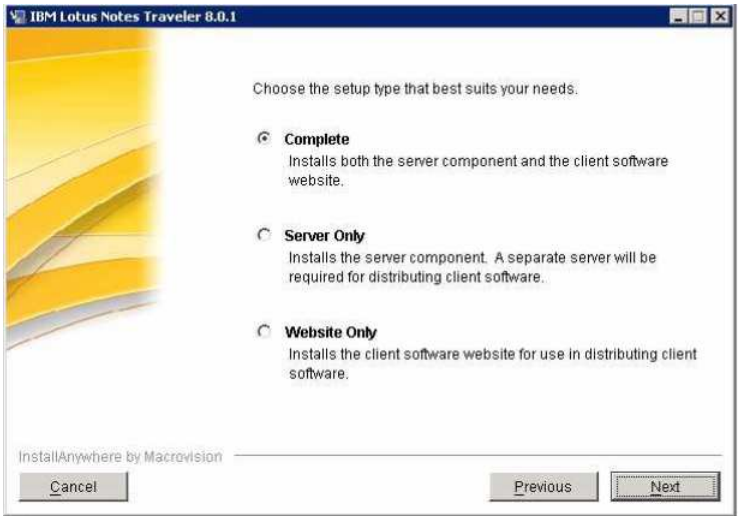


Obrázek 5.22 - Nastavení managera v ACL

5.2.7 Lotus Traveler instalace a nastavení

Pro synchronizaci pošty mezi klientem a mobilním telefonem zvolíme Lotus Traveler. A to z důvodů, že používáme Lotus Notes a Lotus Dominu verze 8, ve které je Lotus Traveler součástí licence a je ho po nainstalování na server možno bezplatně využívat.

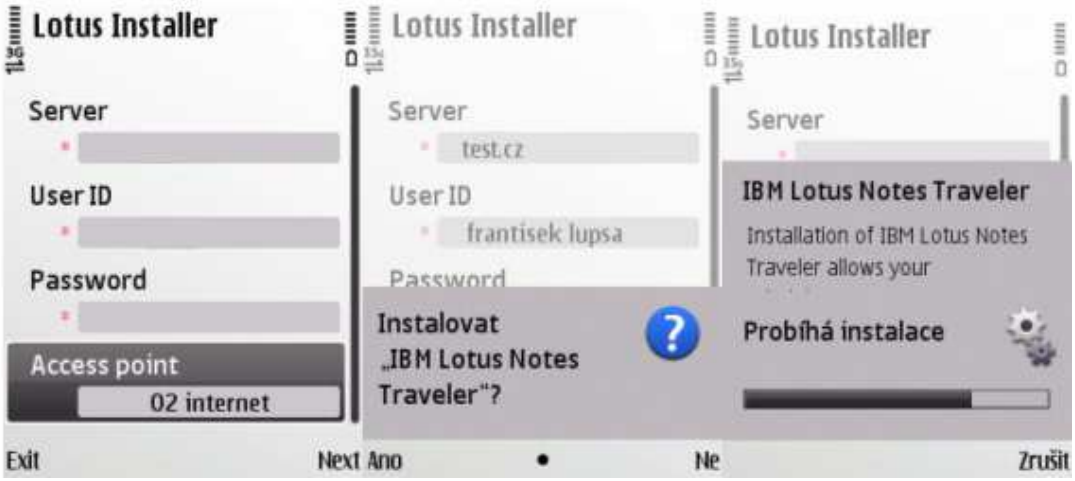
Zvolíme kompletní instalaci, která nainstaluje Lotus Traveler server a webové stránky, na které se umístí instalační balíčky Traveleru pro mobilní zařízení. Uživatel si tam bude moci po přihlášení na příslušný web balíček stáhnout a nainstalovat do svého mobilního zařízení. Traveler podporuje telefony využívající Symbian S60+, Windows Mobile 5+ či Apple iPhone.



Obrázek 5.23 - Instalace LN Traveler

Instalace i celý provoz Lotus Traveleru probíhá pomocí mobilního zařízení. Pro práci je tedy vhodné mít aktivován datový tarif, nebo mít dostupné WiFi připojení.

V nastavení vyplníme server na kterém je Traveler nainstalován. Jako User ID zvolíme naše LN jméno a zadáme heslo do klienta Lotus Notes.
Instalaci zahájíme stažením instalačního souboru z Traveler serveru. Po úspěšném stažení můžeme zahájit samotnou instalaci. Z důvodu vyšší bezpečnosti nastavíme firewall. Pro přístup na něj tedy musíme ještě naistalovat VPN klienta pro přístup do podnikové sítě. Instalační balíček VPN klienta umístíme spolu s instalační sadou Travelera na server.

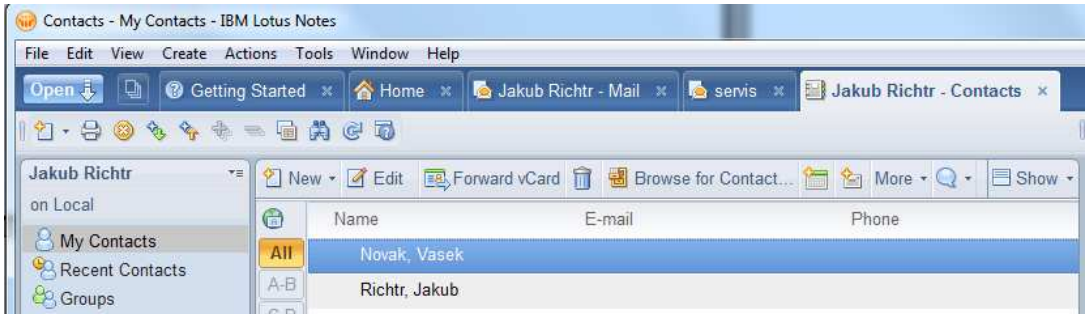


Obrázek 5.24 - Instalace Traveleru v mobilu

Po úspěšné instalaci je třeba Traveler nakonfigurovat. Dosavadní položky kalendáře v telefonu budou odstraněny. Kontakty je možné nahradit nebo doplnit. Nastavíme tedy synchronizaci pro všechny položky. Synchronizaci jedné z položek emailů, kalendáře, kontaktů nebo poznámek lze vypnout nejen při konfiguraci ale i dodatečně. Dále nastavíme automatickou synchronizaci v nastavení Traveleru zvolíme Auto Sync a nastavíme Schedule na hodnotu always connected. V položce Zprávy se nám nyní objeví ikona Lotus Traveler.

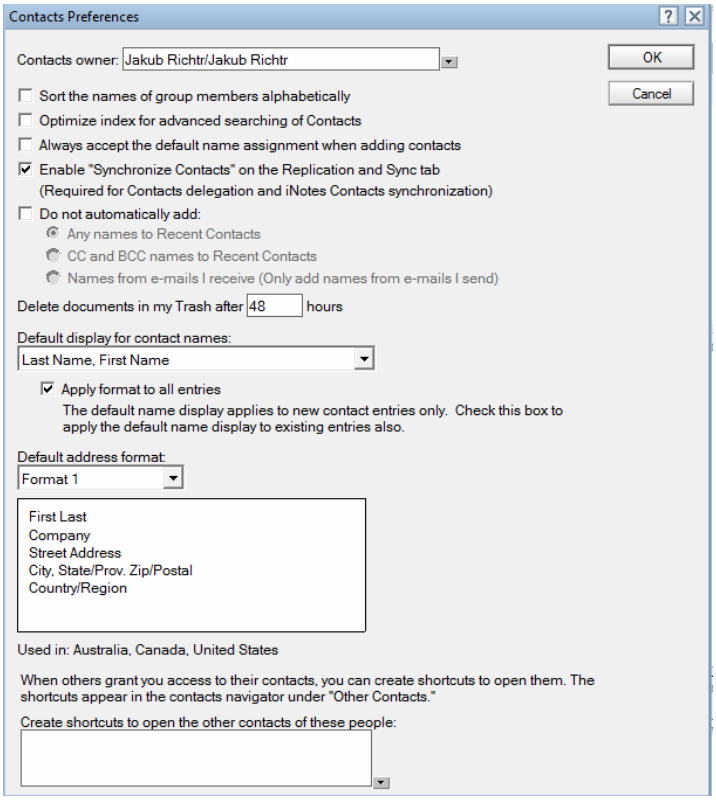
Obrázek 5.25 - Konfigurace Traveleru v mobilu

Po dokončení instalace a konfigurace mobilního telefonu je třeba nastavit replikaci a synchronizaci v klientu Lotus Notes. Toto nastavení provedeme pomocí iNotes. Prvním krokem je povolení synchronizace kontaktů. Otevřeme databázi names.nsf, kde se nachází naše osobní kontakty, a zvolíme Preference.



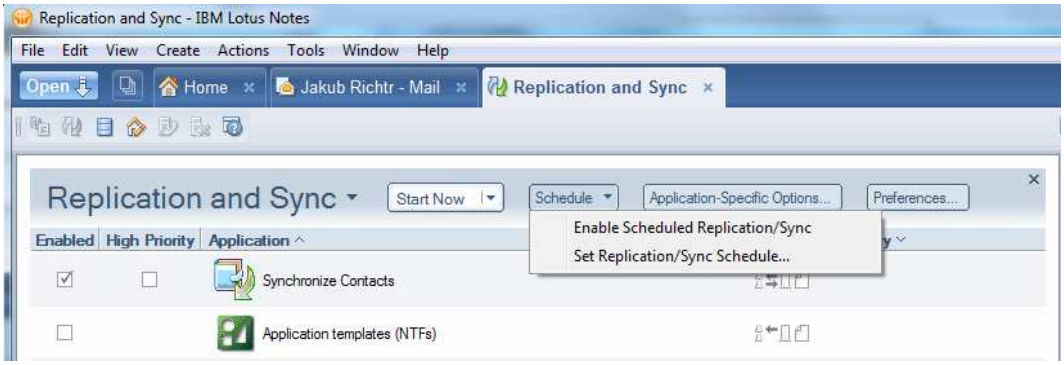
Obrázek 5.26 - Výběr uživatele v kontaktech

V Contact Preferences povolíme synchronizaci kontaktů v replikátoru, což je vyžadováno v případě synchronizace kontaktů aplikace iNotes.



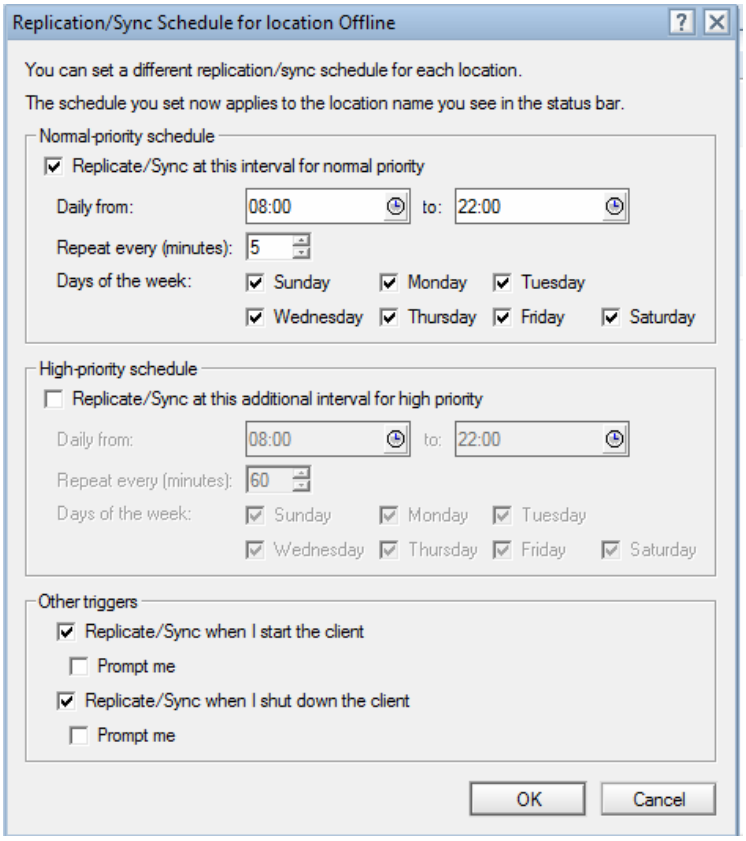
Obrázek 5.27 - Nastavení synchronizace

Následně nastavíme replikace. Otevřeme okno replikace *File-Replication-Options* a v něm vybereme možnost synchronizace kontaktů a zvolíme Schedule pro nastavení plánu replikace.



Obrázek 5.28 – Volba replikace

V nastavení plánu replikace vybereme plán s normální prioritou. V něm nastavíme opakování vždy po 5 minutách, tento interval by měl být pro náš účel dostačující. Dále ještě nastavíme, aby se replikace prováděla vždy při spuštění a ukončení klienta. U volby pro ukončení je ještě vhodné zaškrtnout možnost dotazu (Promt me). Je to vhodné v případě, že provedeme změny, které nechceme ihned replikovat.



Obrázek 5.29 - Nastavení replikace a synchronizace

5.2.6 Webové rozhraní

Do webového rozhraní se přihlásíme přes webový prohlížeč, plně podporovaný je Internet Explorer. Webové rozhraní však bez problému běží i v Mozilla Firefoxu a dalších prohlížečích. Po zadání adresy webového serveru je uživatel přesměrován na zabezpečený protokol https a musí přijmout, stáhnout a nainstalovat potřebné certifikáty. Šablona webového rozhraní od verze 8 je plnohodnotnou náhradou klienta Lotus Notes a uživatel zde najde veškeré potřebné funkce. Po přihlášení zvolíme v záložce Předvolby možnost Zabezpečení. Zde je nutné spustit import ID, abychom mohli pracovat s námi zašifrovanými maily a databázemi a dále používat šifrování uživatelským ID. Je zde možno nastavit heslo pro www přístup, které tak může být odlišné od hesla v ID do klienta. Heslo pro www přístup můžeme samozřejmě nastavit i v klientu. Otevřeme databázi uživatelů na příslušném serveru (Seznam adres) vybereme svůj účet a přes *Actions-Othes-Set www password* nastavíme heslo.

5.3 Shrnutí

Následujícím nastavením Lotus Notes, které bylo provedeno v praktické části, se podařilo splnit zadané požadavky. Při řešení problematiky a následném testování se však objevila i řada drobných problémů.

5.3.1 Navržené řešení

- Pro řešení je zvolen server Lotus Domino 8.5 a klient Lotus Notes 8.5
- Vytvořen uživatelský účet - vygenerováno ID a vytvořena poštovní databáze na serveru
- Nastaveno základní uživatelské zabezpečení včetně potřebného šifrování
- Přidán elektronický podpis
- Nastavena kapacita schránky na 300MB včetně nastavení prahu varování při 250MB k upozornění uživatele o možnosti archivace
- Nastavena archivace včetně nastavení zabezpečení archivu
- Nastavení delegování přístupových práv pro možnost sdílení mailů, kalendáře či úkolů mezi uživateli
- Pro přístup k poště z mimopodnikové sítě je zřízena možnost přístupu přes VPN a přístup přes webové rozhraní
- Pro možnost okamžité blokace uživatele je zřízena skupina DenyAccess
- Vytvořena zástupná schránka a poštovní databáze na serveru pro pracovníky servisu. Po přijetí e-mailu se ihned v e-mailu zobrazí jméno uživatele, který ho přijal.
- Nastavena požadovaná hierarchie přístupových práv uživatelů v zástupné schránce
- Pro přístup přes mobilní telefon byl zvolen Lotus Traveler, který je bezplatnou součástí verze 8.5

5.3.2 Zjištěné nedostatky

- Velká náročnost na operační paměť, zejména při nastavení replikací velmi dlouhé startování systému
- Při prostém smazání pravidla ze seznamu zůstane pravidlo nadále aktivní bez varování uživatele
- Nekompatibilita webového rozhraní iNotes s Mozzila Firefox 4
- Velikost poštovní databáze se i po odmazání pošty neprojeví v reálném čase a uživatel nemá možnost spustit manuálně optimalizaci své databáze na serveru
- Problém s nedoručením e-mailů s elektronickým podpisem při užití českých verzí klienta
- V případě, že se neužívá ID Vault nastávají možné problémy při manipulaci s uživatelským ID a to například při jeho obnově
- Nekompatibilita klientů verze Lotus Notes 7 a starších s operačními systémy Windows Vista a Windows 7

5.4 Porovnání Lotus Notes s alternativami

Vzhledem k tomu, že v současné době je na trhu pouze Microsoft, který svými produkty může IBM a jejich Lotus Notes konkurovat, zaměříme se pouze na porovnání mezi produkty těchto dvou firem. Pro porovnání je tedy zvolena aktuální verze klientu firmy IBM Lotus Notes R8.5 a serveru Lotus Domino stejné řady. A klient Outlook 2007 a server Exchange 2010 společnosti Microsoft. Jelikož IBM se svými Lotus Notes soustřeďuje zejména na bezpečnost, nemělo by porovnávání pouze v této oblasti smysl. Proto se zaměříme i na ostatní výhody a nevýhody jednotlivých produktů.

	Lotus Notes R8.5/Lotus Domino 8	Outlook 2007/MS Exchange 2010
Bezpečnost	Vysoká odolnost proti běžným útokům	Průměrná odolnost proti běžným útokům
	Vysoká odolnost proti virům	Průměrná odolnost proti virům
	Snadné nastavení oprávnění přístupu uživatelů/adminů k datům	Obtížné nastavení oprávnění přístupu uživatelů/adminů k datům
	Možnost sledování logů aktivit na serveru v reálném čase	Možnost sledování logů aktivit na serveru pouze zpětně
Ostatní	Průměrná podpora a rozšíření v EU	Vysoká podpora a rozšíření v EU
	Snadná instalace, zálohování a obnova	Náročná instalace, zálohování a obnova
	Nezávislý na OS	Závislý na Microsoft OS
	Průměrně přívětivé uživatelské prostředí	Vysoce přívětivé uživatelské prostředí
	Snadná tvorba aplikací na míru	Náročná tvorba apliakcí na míru
	Nutnost jednotlivé licence pro každého klienta	Různé individuální řešení licencí dle zákazníka
	Průměrná podpora kancelářských aplikací (Lotus Symphony)	Vysoká podpora kancelářských aplikací (MS Office)

Tab. č.1 – Porovnání Lotus Notes a MS Exchange

Z tabulky je patrné, že v oblasti bezpečnosti se s Lotusem nemohou rovnat ani produkty firmy Microsoft. Lotus poskytuje vysokou úroveň odolnosti proti útokům a virům. Mezi jeho hlavní znaky patří zejména Notes ID, bez kterého se uživatel do klienta nedostane. Další velkou výhodou je možnost snadného nastavění ať již ACL nebo ECL pro přidělování uživatelských práv k účtům, databázím či aplikacím. Neméně důležité je i kompletní logování a možná okamžitá reakce na bezpečnostní problémy zejména díky naprogramovaným agentům, kteří administrátory okamžitě informují například při zvýšeném pokusu o neoprávněný přístup do databáze.

V ostatních oblastech hodnocení má Lotus navrch především v možnosti tvorby vlastních aplikací přímo na míru ve vývojovém prostředí Lotus Designer a ve snadné instalaci a celkové údržbě systému.

MS Outlook naopak získává body ve vysoké podpoře pro uživatele, produkty firmy Microsoft jsou nejrozšířenějšími v Evropě a velká většina uživatelů je zná a umí s nimi pracovat. Dalším kladem je velmi přívětivé uživatelské prostředí, které se snaží IBM dohánět, nicméně Microsoft je zde stále napřed a nabízí lepší design aplikací. Kladem je také propojení s kancelářskými aplikacemi MS Office. Lotus nabízí alternativu v kancelářských aplikacích Lotus Symphony ty však kvalit MS Office nedosahují zejména díky velkému rozšíření MS Office u uživatelů. Microsoft také nabízí možnost individuálního přístupu k zákazníkům ohledně licencí, nabízí různá řešení pro své klienty. U Lotus Notes je potřeba zakoupil licenci k jednotlivým klientům.

6 Závěr

V současnosti nemá Lotus Notes v oblasti bezpečnosti příliš konkurenci. Vyznačuje se zejména vysokou odolností proti útokům a virům. Charakteristickým znakem pro Lotus Notes je Notes ID, což je něco jako elektronický průkaz, fyzicky reprezentovaný malým souborem na pevném disku, USB flash disku či jiném médiu. Tento soubor musí uživatel použít vždy, když chce pracovat s klientem Lotus Notes. Další faktory zajišťující bezpečnost jsou certifikáty, Access Control List pro správu přístupových práv či logy, které umožňují okamžitou reakci na případné nebezpečí.

Hlavním cílem vlastní práce bylo navrhnout řešení v Lotus Notes dle zadání, včetně ukázky možného nastavení klienta. A tím tak demonstrovat možnosti využití Lotus Notes. Požadavky na systém jsem zvolil na základě konzultace s vedoucím pracoviště servisu, aby se jednalo o reálné požadavky na poštovní systém využitelné v praxi. Při návrhu řešení byl kladen důraz zejména na možnosti nastavení zabezpečení v klientu Lotus Notes. Pro řešení byl vybrán klient Lotus Notes 8.5R a server Lotus Domino stejné série. Na stejný server byl nainstalován i Lotus Traveler, který je součástí verze 8.5 a byl tak použit pro mobilní řešení.

Po zřízení uživatelského účtu a jeho nastavení, byl nainstalován a nakonfigurován klient Lotus Notes dle předem stanovených požadavků. V uživatelském účtu bylo nastaveno základní zabezpečení včetně šifrování, nastavena archivace, možnost delegování a elektronický podpis. Dále byla zřízena zástupná schránka pro účely pracovníků servisu. Šablona zástupné schránky zajistí požadovanou funkčnost, aby se po přijetí e-mailu ihned u daného e-mailu zobrazilo jméno uživatele, který ho přijal. Pro přístup přes mobilní telefon byl zvolen Lotus Traveler, který je součástí verze 8.5. Traveler byl následně nainstalován a nastaven. K přístupu k poště z mimopodnikové sítě je zajištěn přístup přes VPN, který umožní užívání klienta i v případě že uživatel není v doméně. Další alternativou je webový přístup, který je pro tyto účely nakonfigurován s šablonou, která plnohodnotně nahrazuje klienta.

Celá práce s nastavením klienta probíhala bez větších problémů. Ovládání je vcelku intuitivní a zvládne ho i člověk bez velkých zkušeností z LN. Dobře udělaný je zejména

Access Control List, ve kterém se dají opravdu snadno nadefinovat požadovaná oprávnění v databázích či aplikacích pro jednotlivé uživatele. Obdobné nastavení může i sám uživatel udělat v editoru pro delegování přístupových práv, který je s ACL propojen.

První problém jsem zaznamenal při tvorbě pravidel. Po vytvoření pravidla se toto pravidlo ihned samo aktivuje. V případě, že chceme pravidlo vypnout, je nutné ho nejprve deaktivovat a až poté smazat. Pokud uživatel pravidlo ze seznamu smaže, aniž by ho předtím deaktivoval, pravidlo zůstane aktivní a uživatel již nemá možnost ho bez pomoci administrátora deaktivovat. Dalším negativem je pro uživatele velká náročnost klienta na operační paměť, je tedy třeba opravdu výkonný počítač. Jelikož při startu a ukončování probíhají replikace, může zprovoznění klienta trvat i několik minut, což je pro uživatele nepříjemné. Problém nastává i při využití nové verze Mozilla Firefox 4, který nepodporuje webové rozhraní Lotus Notes. Velké množstvi bezpečnostních problému vyřešilo zavedení zabezpečeného trezoru ID Vault. Jeho problémem je však možnost použití pouze od verze 8.5 pro uživatele, kteří mají starší licenci Lotus Notes, tato alternativa stále není možná. Mezi podobné problémy lze zařadit i nekompatibilita klientu Lotus Notes verze 7 a starších verzí s operačními systémy Windows Vista a Windows 7. V případě přechodu na tyto systémy je třeba zakoupti licence i pro produkty Lotus Notes verze 8.

V závěru práce bylo provedeno menší porovnání Lotus Notes s jeho alternativami. Pro porovnání byl zvolen klient Outlook 2007 a server Exchange 2010 společnosti Microsoft, který je v současné době jedinou srovnatelnou konkurencí pro Lotus Notes. I přesto však v porovnání bezpečnosti Lotus Notes jasně dominuje. Při porovnávání ostatních faktorů však již Lots Notes, který se specializuje zejména na svou bezpečnost, neměl vždy navrch. MS Outlook získal převahu ve vysoké uživatelské podpoře, jelikož produkty firmy Microsoft jsou nejrozšířenějšími v Evropě a velká většina uživatelů je zná a umí s nimi pracovat. Dalším kladem je také propojení s kancelářskými aplikacemi MS Office a uživatelsky přívětivé prostředí a líbivý design.

7 Seznam použitých zdrojů

[1] DAHM, F. a kol. *Security Considerations in Lotus Notes and Domino 7*, IBM Redbooks, 2006. ISBN 0738497347.

[2] LANDON a kol. *iNotes Web Access on the IBM iSeries Server*, IBM Redbooks, 2002. ISBN 0738425206.

[3] MORAVEC, L.: *Lotus Notes 7 uživatelská příručka*, Grada, 2008, 255 str., ISBN 978-80-247-2346-4.

[4] TWOREK, W. a kol. *Lotus Security Handbook*, IBM Redbooks, 2004. ISBN 0738498467.

[5] Ortex. *Lotus Domino Express* [online]. [cit.2011-01-22]. URL: <http://lotus.ortex.cz/lotus-domino-express.aspx>.

[6] Wikis. *E-mailový klient* [online]. [cit.2011-02-22]. URL: <http://cs.wikipedia.org/wiki/E-mailov%C3%BD_klient>.

[7] DALEKOREJ, V. *BlackBerry Enterprise Server* [online]. [cit.2011-03-08]. URL: <http://blackberryczech.cz/?p=3926>.

[8] PLCH, E. *Lotus Knows* [online]. [cit.2011-02-20] URL: <http://www-05.ibm.com/cz/events/symposium2010/pdf/Lotus_software_pro_BlackBerry_-_System4u.pdf>.

[9] KUNC, P. *Lotus Notes Traveler 8.5.1* [online]. [cit.2011-03-22] URL: <http://petrkunc.net/lotus/1256244806-lotus-notes-traveler-851-prirucka-uzivatele.html>.

[10] KUNC, P. *Seriál Lotus Notes: Bezpečnost* [online]. [cit.2011-03-10] URL: <http://petrkunc.net/lotus/1254431729-serial-lotus-notes-bezpecnost.html>.

[11] TUROŇ, R. *Lotus Notes R8.5* [online]. [cit.2011-01-11] URL: <http://www.tcl-digitrade.com/>.

[12] KUNC, P. *iNotes Lite* [online]. [cit.2011-01-20] URL: <http://petrkunc.net/lotus/1114114627-inotes-lite.html>.

[13] LICHTENBERG, A. *Lotus Traveler Security* [online]. [cit.2011-01-13] URL: <http://www.sutol.cz/sutol/sutol.nsf/c4e424a4a3af0cf0c12574ac002bd0e6/e70079bc258fb873c12576ff007f2318?OpenDocument&Highlight=0,Traveler>.

[14] KUNC, P. *Bezpečnost v Lotus Notes* [online]. [cit.2011-01-28] URL: <http://petrkunc.net/lotus/1188342511-clanek-bezpecnost-v-lotus-notes.html>.

[15] KUNC, P. *Seriál Lotus Notes: ACL (1.)* [online]. [cit.2011-01-19] URL: <http://petrkunc.net/lotus/1255986797-serial-lotus-notes-acl-1.html>.

[16] KUNC, P. *Seriál Lotus Notes: ACL (2.)* [online]. [cit.2011-01-28] URL: <http://petrkunc.net/lotus/1262023152-serial-lotus-notes-acl-2.html>.

[17] POKORNY, R. *ID Vault &Shared Login* [online]. [cit.2011-02-05] URL: <http://www.sutol.cz/sutol/sutol.nsf/0/2B8F55AB211F07BAC125766D0049BC4D/$FILE/IDVault.pdf>.

[18] Microsoft. *Porovnání produktů Lotus Domino/Notes a Exchange Server 2010*. [online]. [cit.2011-03-03] URL: <http://www.microsoft.com/cze/exchange/product-information/compare/notes.aspx>.

[19] Sybase. *Onebridge Mobile Groupware* [online]. [cit.2011-02-20] URL: <http://www.sybase.cz/index.php?option=com_content&view=article&id=5&mid=34>.

[20] NAVRÁTIL, R. *Lotus Notes Traveler 8.5.2 a novinky* [online]. [cit.2011-01-28] URL:<http://www.sutol.cz/sutol/sutol.nsf/0/CC3B6548609F43E5C125779000830F32?Opendocument>.

[21] Whitesoft. *Analýza nákladů* [online]. [cit.2011-02-22] URL: <http://www.lotus-katalog.cz/img/whitesoft/Analyza%20nakladu%20SMB40.pdf>.

Seznam obrázků

Obrázek 5.1 - Vytvoření nové databáze 38
Obrázek 5.2 - Nastavení šifrování 39
Obrázek 5.3 - Nastavení quoty mailboxu 39
Obrázek 5.4 - Nastavení ACL 40
Obrázek 5.5 - Nastavení ECL 41
Obrázek 5.6 - Zadání vlastníka v předvolbách 41
Obrázek 5.7 - Uživatelské předvolby - automatický podpis 42
Obrázek 5.8 - Uživatelské předvolby - šifrování 43
Obrázek 5.9 - Automatické zamykání klienta 43
Obrázek 5.10 - Volba síly šifrování hesla ID 44
Obrázek 5.11 – Šifrování u portu TCP/IP 45
Obrázek 5.12 - Tvorba pravidla 46
Obrázek 5.13 - Delegování práv 47
Obrázek 5.14 - Tvorba archivu 48
Obrázek 5.15 - Nastavení kriterií archivace 48
Obrázek 5.16 - Šifrování archivu 49
Obrázek 5.17 - Vytvoření skupiny 50
Obrázek 5.18 - Nastavení skupiny 50
Obrázek 5.19 - Skupina pro blokování uživatelů 51
Obrázek 5.20 - Náhled zástupné schránky 51
Obrázek 5.21 – Přidání skupiny do ACL 52
Obrázek 5.22 - Nastavení managera v ACL 53
Obrázek 5.23 - Instalace LN Traveler 54
Obrázek 5.24 - Instalace Traveleru v mobilu 55
Obrázek 5.25 - Konfigurace Traveleru v mobilu 56
Obrázek 5.26 - Výběr uživatele v kontaktech 57
Obrázek 5.27 - Nastavení synchronizace 57
Obrázek 5.28 – Volba replikace 58
Obrázek 5.29 - Nastavení replikace a synchronizace 58