Kupní smlouva
uzavřená dle § 409 a následujících obchodního zákoníku (zákon č. 513/91 Sb.) a dle zákona č. 121/2000 Sb. v platném znění

Článek 1

Smluvní strany

Objednatel:

	Statutární město Brno
Zastoupené:	Bc. Romanem Onderkou, MBA, primátorem
Se sídlem:	Dominikánské náměstí 196/1
	601 67 B r n o
IČ:	44992785
DIČ:	CZ44992785
Bankovní spojení:	The Royal Bank of Scotland plc, organizační složka
Číslo účtu:	7510006658/5400
Ve věcech technických je oprávněn jednat:	Ing. Jaromír Emmer, vedoucí OMI MMB
Ve věcech smluvních je oprávněn jednat:	Ing. Robert Kotzian, Ph.D., 1. náměstek primátora
Číslo smlouvy:	5312025490

Zhotovitel:

Společnost:	M-COM LAN solution, spol. s r.o.
Jednající:	Radek Erben
Se sídlem:	Pod Viaduktem 647/51
	155 00 Praha - Stodůlky
IČ:	25672959
DIČ:	CZ25672959
Zapsána v OR, vedeném	u Městského soudu v Praze
Bankovní spojení:	Raiffeisenbank a.s.
Číslo účtu:	19100001/5500
Ve věcech technických je oprávněn jednat:	Jaroslav Techl, produkt manager
Ve věcech smluvních je oprávněn jednat:	Jiří Jiskra, account manager
Číslo smlouvy:	

Pro účely této Smlouvy se uvedené smluvní strany označují jako Objednatel a Zhotovitel. Dále společně strany a jednotlivě strana.

Článek 2

Předmět Smlouvy

2.1 Předmětem této Smlouvy je dodávka licencí SW produktu k zajištění antivirové a antispyware ochrany pro 1400 klientů (server, workstation, notebook) a to včetně propojení s prostředky personálního firewallu pro zabezpečení jednotlivých PC Objednatele před možnými útoky virů a dalším útokům zejména z prostředí Internetu, včetně centrální vzdálené správy z jednoho místa. Předmětem plnění veřejné zakázky je rovněž instalace SW produktu na HW Objednatele (instalaci provede zaměstnanec Objednatele pod kontrolou pracovníka Zhotovitele). Bližší specifikace předmětu plnění Smlouvy je uvedena v Příloze č. 1 a v Příloze č. 2 Smlouvy.

2.2 Zhotovitel prohlašuje, že je oprávněn k prodeji výše uvedených produktů, které jsou předmětem plnění Smlouvy a na základě toho poskytuje Objednateli právo užívat všechny ve Smlouvě uvedené produkty. Doba užívání produktu bude ode dne podpisu Smlouvy oběma smluvními stranami na dobu neomezenou, služby budou poskytovány na dobu 36 měsíců.

Článek 3

Termín a místo plnění předmětu Smlouvy

3.1 Zhotovitel se zavazuje k dodávce předmětu plnění Smlouvy do 30 pracovních dnů ode dne podpisu této Smlouvy.

3.2 Místem plnění předmětu Smlouvy je budova Magistrátu města Brna, Malinovského nám. 3, Brno. O předání předmětu plnění sepíší smluvní strany akceptační protokol.

Článek 4

Cena

4.1 Cena za plnění za dobu 12 měsíců dle čl. 2 bodu 2.1 a 2.2 této Smlouvy je stanovena na základě dohody obou smluvních stran dle následující tabulky ve výši:

Cena za plnění za dobu	Položka nabídkové ceny	Počet ks	Cena včetně DPH	DPH 21%	Cena bez DPH
prvních 12-ti měsíců	Pořizovací cena licencí včetně podpory na 12 kalendářních měsíců plus implementační práce	1400ks 5MD	448 910 Kč	77 910 Kč	371 000 Kč
druhých 12-ti měsíců	Zakoupení podpory na druhý rok - 12 kalendářních měsíců	1400ks	49 126 Kč	8 526 Kč	40 600 Kč
třetích 12-ti měsíců	Zakoupení podpory na třetí rok - 12 kalendářních měsíců	1400ks	49 126 Kč	8 526 Kč	40 600 Kč

4.2 Cena stanovená v odst. 4.1 je cenou nejvýše přípustnou za plnění předmětu Smlouvy, včetně všech poplatků a veškerých dalších nákladů s plněním předmětu Smlouvy souvisejících.

4.3 V případě jiné sazby DPH bude Zhotovitel Objednateli účtovat sazbu DPH ve výši odpovídající platným a účinným právním předpisům. Cena za plnění bez DPH tímto není dotčena.

Článek 5

Platební podmínky

5.1 Daňový doklad bude mít splatnost 30 dnů od data doručení Objednateli. Objednatel bude hradit cenu za plnění předmětu Smlouvy ve 12 měsíčním intervalu po celou dobu platnosti smlouvy. Faktury budou pokládány za uhrazené dnem odepsání fakturované částky z účtu Objednatele.

5.2 Všechny daňové doklady musí obsahovat náležitosti stanovené zákonem č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů. V případě, že faktura nebude mít odpovídající náležitosti, je Objednatel oprávněn zaslat ji ve lhůtě splatnosti zpět Zhotoviteli k doplnění, aniž se tak dostane do prodlení se splatností. Zhotovitel vystaví znovu daňový doklad a sjednaná lhůta splatnosti počíná běžet znovu od opětovného doručení náležitě doplněného či opraveného dokladu.

5.3 Zhotovitel vystaví Objednateli první daňový doklad na cenu za 12 měsíců plnění předmětu Smlouvy do jednoho měsíce od podepsání akceptačního protokolu oběma smluvními stranami. Zhotovitel vystaví Objednateli druhý daňový doklad na cenu za dalších 12 měsíců plnění předmětu Smlouvy do jednoho měsíce od prvního výročí platnosti Smlouvy. Zhotovitel vystaví Objednateli třetí daňový doklad na cenu za dalších 12 měsíců plnění předmětu Smlouvy do jednoho měsíce od druhého výročí platnosti Smlouvy.

Článek 6

Záruka za jakost

6.1 Zhotovitel zaručuje Objednateli technickou podporu předmětu plnění po celou dobu trvání Smlouvy.

6.2 Zhotovitel má uzavřenou pojistnou Smlouvu ke krytí škod, způsobených v souvislosti s jeho činností na výši pojistného plnění 2.000.000 Kč (slovy: dvamilionykorunčeských). Zhotovitel je povinen toto pojištění udržovat po celou dobu platnosti této Smlouvy.

Článek 7

Smluvní pokuty a sankce

Smluvní strany se dohodly, že:

7.1 V případě prodlení Objednatele s plněním peněžitého závazku Objednatel uhradí úrok z prodlení ve výši 0,05 % z dlužné částky za každý i započatý den prodlení maximálně však 10 % p. a.

7.2 V případě prodlení Zhotovitele, s dodáním předmětu Smlouvy, Zhotovitel uhradí smluvní pokutu za prodlení s plněním ve výši 0,05 % z ceny včas nedodaného předmětu Smlouvy za každý i započatý den po termínu plnění dle článku 3 této Smlouvy.

7.3 V případě prodlení Zhotovitele s provedením díla delším než jeden měsíc má Objednatel právo od Smlouvy odstoupit. V tomto případě nemá Zhotovitel nárok na úhradu jakýchkoliv plnění.

7.4 Ustanovením o smluvní pokutě není dotčeno právo na náhradu škody.

Článek 8

Závěrečná ustanovení

8.1 Tato Smlouva nabývá platnosti a účinnosti dnem jejího podpisu oběma smluvními stranami.

8.2 Ustanovení obsažená v těle Smlouvy mají v případě výkladových nejasností přednost před ustanoveními obsaženými ve všeobecných obchodních podmínkách Zhotovitele.

8.3 Smlouvu lze měnit či doplňovat pouze písemnými dodatky odsouhlasenými oběma smluvními stranami.

8.4 Objednatel má právo Smlouvu vypovědět bez udání důvodu k datu výročí podpisu Smlouvy, v tříměsíční výpovědní lhůtě, která začíná běžet prvním dnem následujícího měsíce po doručení výpovědi Zhotoviteli.

8.5 Tato Smlouva je vyhotovena ve čtyřech vyhotoveních, z nichž dvě vyhotovení obdrží Objednatel a dvě vyhotovení obdrží Zhotovitel.

8.6 Záležitosti v této Smlouvě výslovně neupravené se řídí příslušnými ustanoveními obchodního zákoníku v platném znění.

8.7 Objednatel i Zhotovitel se zavazují vzájemně informovat o všech organizačních změnách (název, sídlo tel., fax., apod.)

8.8 Zhotovitel i Objednatel jsou povinni zachovat mlčenlivost o všech skutečnostech, údajích a informacích, týkajících se druhé strany, které mají povahu jejich obchodního tajemství v rozsahu a za podmínek §17 obchodního zákoníku, a o kterých se dozví v souvislosti s plněním této Smlouvy. Zhotovitel i Objednatel se zavazují, že tyto skutečnosti nesdělí

ani jiným způsobem neposkytnou žádné třetí osobě a zajistí jejich přiměřenou ochranu a utajení.

8.9 Zhotovitel je dle zákona č.101/2000Sb., o ochraně osobních údajů, v platném znění povinen zachovávat mlčenlivost o osobních údajích a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů v informačním systému Objednatele. Povinnost mlčenlivosti trvá i po ukončení platnosti Smlouvy. Zhotovitel odpovídá Objednateli v plné míře za škodu, kterou mu způsobí porušením tohoto ustanovení.

8.10 Objednatel je povinen respektovat skutečnost, že zhotovitel musí být oprávněn dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, v platném znění, určité informace zveřejnit (§ 9 odst. 2 cit. zák.). Ostatní informace uvedené ve Smlouvě či získané na základě Smlouvy budou stranami považovány za obchodní tajemství podle obchodního zákoníku, pokud je právně možné je jako obchodní tajemství kvalifikovat.

8.11 Zhotovitel bere na vědomí povinnost Objednatele, vyplývající ze zákona, uveřejnit uzavřenou Smlouvu k předmětné veřejné zakázce na profilu Objednatele, a s uveřejněním této Smlouvy souhlasí.

8.12 Nedílnou součástí této Smlouvy jsou:

Příloha č. 1 – A. Požadavky na antivirový systém pro MMB
B. Bližší specifikace předmětu plnění Smlouvy

Tato Smlouva byla schválena Radou města Brna na schůzi R6/094 dne 30. 1. 2013.

V Brně dne 15 -03- 2013

Za Objednatele:

.....

za statutární město Brno
1. náměstek primátora
Ing. Robert Kotzian, Ph.D.

V Praze dne 11. 3. 2013

Za Zhotovitele:

.....

za M-COM LAN solution, spol s r.o.
jednatel
Radek Erben

Příloha č. 1 – A. Požadavky na antivirový systém pro MMB

1. Požadavky na centrální vzdálenou správu z jednoho místa

Obsahuje: antivir, antispyware, firewall
Počet klientů: 1400
Platformy: server, workstation, notebook
Management:

- centrální správa, dálková instalace klientů na stanicích prostřednictvím administrátorské konzoly,
- reporty: možnost nastavení požadovaných reportů administrátorem,
- skenování komprimovaných a archivních souborů,
- možnost lokální instalace na stanici (selfmanaged verze),
- možnost vytváření instalačních balíčků podle požadavků administrátora.

Update virových definic:

- automatický update definic,
- manuální update definic.

Help/Support: minimálně email support.y

Podporované platformy:
Windows XP (32 bit), Windows 7 (32 a 64 bit), Windows Servers 2003, 2008 a novější.

Firewall:
Zahrnuje vnitřní firewall umožňující blokovat neautorizované přístupy a naopak povolit požadovanou komunikaci.
Možnosti nastavení:
a) centrální konfigurace pravidel administrátorem,
b) pro vybrané skupiny (např. IT oddělení):
- možnost lokální konfigurace,
- možnost snadno na stanici dohledat v logu aplikaci, která má zablokovanou komunikaci a pokud se o ní s jistotou ví, že je bezpečná, tak ji povolit.

2. Požadavky na klienty

Možnosti ochrany: antivir, antispyware, firewall
Počet klientů: 1400

Skenování při přístupu - soubory jsou automaticky skenovány při přístupu nebo jejich přijímání.
Skenování na vyžádání - skenování souboru nebo složky na vyžádání.
Plánované skenování - integrovaný plánovač dovolí skenovat v určeném čase nebo intervalu.
Spyware skenování - obsahuje technologie, zabraňující sběru informací uživatele bez jeho dovolení.
Možnost nastavení, aby program automaticky vyčistil, dal do karantény nebo odstranil infikované soubory bez zásahu uživatele, resp. administrátora.
Možnost umístění infikovaných a potenciálně nebezpečných souborů do karantény, dokud administrátor neurčí způsob zásahu.

Monitorování a skenování síťového provozu v reálném čase sloužící k ochraně proti nebezpečným souborům a odkazům.
Kontrola souborů přicházejících prostřednictvím protokolu POP3. Podpora emailových klientů Microsoft Outlook ve verzích 2003, 2007 a 2010.

3. Ostatní požadavky

Pokud systém ke svému provozu potřebuje SQL server, musí být součástí této nabídky i licence na tento SQL server pro uvedený počet klientů. Velikost databáze SQL musí být dimenzovaná na 3 roky používání.

Požadujeme ukládat data po dobu platnosti smlouvy. Kompletní logy je potřeba uchovávat po dobu 30 dnů. Jde zejména o základní logy typu: scan a risk, systém (aktualizace virových definic a spouštění a ukončení běhu antiviru na stanici), síťová komunikace na úrovni atack a traffic a zablokování programů.

Centrální správa musí být provozovatelná ve virtuálním prostředí VMware na maximální konfiguraci serveru 6GB RAM, 4 vCPU s OS Windows 2008 R2 EN STD, a to včetně případného SQL serveru.

Předpokládáme kompletní a konečné řešení, které nebude vyžadovat žádné další moduly.

4. Instalace

Instalace SW produktu na HW objednatele (instalaci provede zaměstnanec objednatele pod kontrolou pracovníka zhotovitele). Instalací se rozumí instalace dodávaného antivirového systému včetně SQL serveru (SQL server je součástí instalace i v případě, že se použije free verze SQL).

Příloha č. 1 B: Bližší specifikace předmětu plnění Smlouvy

Nabídka implementace antivirového řešení Symantec Endpoint Protection (SEP)

pro

Magistrát města Brna

1.1. POPIS NAVRHOVANÉHO PRODUKTU

Na základě požadavků zadávací dokumentace je nabízen program Symantec Endpoint Protection (SEP).

Tento produkt pokrývající ochranu všech požadovaných částí informačního systému, konkrétně:

- Ochrana koncových bodů ve vnitřní síti zajištěná produktem Symantec Endpoint Protection 12.1.

Pro přehlednost je navrhovaný produkt a jeho verze uvedena v následující tabulce:

Produkt a verze	Umístění a funkce
Symantec Endpoint Protection 12.1	Antivirová, antispyware, antirootkit, ochrana proti hrozbám nulového dne, antivirová ochrana protokolu POP3,SMTP, IDS/IPS a antivirus pro webové prohlížeče, Personální Firewall, Application and device control ochrana stanic, serverů a notebooků virtualizovaných OS a terminál serverů.

1.1.1. SYMANTEC ENDPOINT PROTECTION 12.1

Symantec Endpoint Protection 12.1 dále jen SEP je nová generace systému pro komplexní ochranu koncových zařízení (servery, stanice, notebooky).

Jedná se o systém, kdy koncoví SEP klienti jsou řízeni pomocí řídící konzoly Symantec Endpoint Protection Manager.

Endpoint Protection Manager zajišťuje tyto základní funkce:

- Instalace/upgrade koncových klientů.
- Sdružování klientů do logických skupin (group).
- Vyrozumívání koncových klientů (logování činnosti, reporting stavů).
- Nastavování a přiřazování politik jednotlivých funkcionalit.

Celkově se koncový klient SEP skládá z těchto ochranných komponent:

- Antivirová a antispywarová ochrana – základní antivirová ochrana založená na virových definicích, nově doplněná o reputační metodu ochrany Insight a pokročilou heuristickou

analýzu SONAR, která slouží jako ochrana před „0 day" útoky, antispyware, antirootkit, antivirová ochrana protokolu POP3,SMTP, antivirus pro webové prohlížeče.

- Personální firewall – systém pro definici a řízení konfigurace příchozí a odchozí komunikace. Obsahuje předdefinovaný set firewallových pravidel, která se dají libovolně dále modifikovat a doplňovat.
- Intrusion Protection System IPS – signaturový systém IPS, který slouží pro detekci a blokování nebezpečných kódů IPS modulem na základě generických i vlastních signatur a to i pro webové prohlížeče.
- Application Control – komponenta pro řízení aplikací (jejich logování spouštění, blokování), monitoring přístupu/zápisu do registry systému atd.
- Device Control – slouží k řízení přístupu či spouštění periferních zařízení na koncovém zařízení. Například umožňuje blokování připojování neautorizovaných USB disků, USB flash klíčenek atd.

Produkt se skládá ze dvou základních komponent.

Základní komponenty:

- SEP Policy Manager.
- SEP Client. nebo SEP Client se spuštěnou funkcionalitou Group Update Provider (GUP)

SEP Policy Manager je hlavní řídící komponenta SEP, která spolu s administrátorskou konzolou slouží pro:

- Administrace
- Vytváření a distribuci politik na skupiny klientů.
- Instalaci klientů.
- Monitoring.
- Reporting.
- Logování
- Distribuce update

Události, konfigurační data a data pro identifikaci škodlivého SW jsou uloženy v databázi.

SEP Client je samotná výkonná aplikace, určená pro ochranu serverů a pracovních stanic, která může být instalována v režimu unmanaged, kdy klient není řízen žádným Policy Managerem (konfigurace se provádí přímo z rozhraní klienta), nebo může být instalován v režimu managed, kdy klient je řízen Policy Managerem, ze kterého přebírá politiky a jemuž zpět posílá události o svém chování.

GUP je funkcionalita kterou je možné provozovat na libovolném z klientů na OS Windows a jedná se o redistribuční bod pro definice. Tento bod je využíván v rámci sítí pro snížení zátěže komunikačních linek.

Administrace je zajištěna jednotnou administrátorskou konzolou, která zajišťuje nejen implementaci klientů a jejich správu, ale taktéž pokročilé monitorování a vytváření výstupů o provozu technologie SEP.

Symantec Endpoint Protection obsahuje dvě administrátorské konzoly, kdy jedna funguje jako JAVA plugin, jehož stažení je umožněno připojením na SEP Policy Manager na portu TCP 9090 a druhá jako Web konzola.

Aktualizace definic systému je možná z Internetu z webových stránek výrobce pomocí metody LiveUpdate. Interně v síti je možné aktualizace šířit pomocí několika metod:

- Aktualizací SEP klientů ze SEP Policy Manageru.
- Aktualizací klientů přímo z Internetu metodou LiveUpdate.
- Aktualizací pomocí lokálního aktualizačního zdroje Group Update Provideru (vhodné zejména pro vzdálené pobočky, které mají slabou konektivitu na centrální SEP Policy Manager).

Vyrozumívání je umožněno na třech úrovních:

- Pomocí administrátorské konzoly, které obsahuje desítky předdefinovaných reportů, které se dají dále upravovat. Tyto reporty poskytují informace:
  - Stav klienta (funkční antivirové komponenty, zapnutý FW, komponenty aktualizovány).
  - Přehled nalezených nebezpečných kódů.
  - Informace o klientském zařízení (operační systém, hardware, IP adresa, hostname apod.).

  Reporty se dají získat na vyžádání v administrátorské konzole, nebo se dá jejich doručení plánovat a reporty se dají zasílat emailem na definované adresy.
- Pomocí grafického rozhraní koncového SEP klienta, kde se informace dají získat na úvodní obrazovce například:
  - Stav jednotlivých funkčních komponent, případné vynucení opravné akce.
  - Stav aktualizací funkčních komponent.
  - Detailní informace z logu (zachycená rizika, komunikace se SEP Policy Managerem atd.).
- Vyrozumívání pomocí dialogových oken na koncových zařízeních, například detekce nalezeného viru, upozornění na zastaralé virové definice, firewallem blokovanou komunikaci nebo aplikaci atd. Záleží na nastavené notifikační politice.
- Produkt je dodáván v mnoha jazykových mutacích včetně české verze a navrhovaná licence umožňuje instalaci libovolné z nich.

1.2. POPIS POŽADOVANÝCH FUNKCÍ SYSTÉMŮ A MOŽNOSTÍ JEJICH ROZŠÍŘENÍ FREKVENCE PRAVIDELNÝCH AKTUALIZACÍ VIROVÝCH ŘETĚZCŮ

1.2.1. FREKVENCE PRAVIDELNÝCH AKTUALIZACÍ VIROVÝCH ŘETĚZCŮ

Typy virových řetězců publikovaných výrobcem

Standardní frekvence vydávání antivirových řetězců je obvykle 1-3x denně.

Možnosti aktualizací navrhovaných produktů

Navrhované produkty lze aktualizovat těmito způsoby:

- Aktualizace LiveUpdate.
- Rapid Release aktualizace.
- Aktualizace pomocí spustitelného souboru.
- Kombinace výše uvedených metod.

Aktualizace LiveUpdate

LiveUpdate utilita je součást každé serverové a klientské části nabízených antivirových produktů.

Tato utilita slouží ke stahování aktualizací přímo z webového sídla výrobce nebo z interního zdroje LiveUpdate (LiveUpdate Administrator) V tomto případě však modul LiveUpdate Administrátor nebude na přání zákazníka vysloveného v zadávací dokumentaci implementován.

Stahování aktualizací utilitou LiveUpdate může být definováno několika způsoby:

- Automatické stahování aktualizací v definovaných intervalech.
- Manuální spouštění aktualizací.
- Kombinace výše uvedených metod.

Při automatickém stahování se dá vymezit okno, ve kterém mají být aktualizace stahovány, opakování v případě neúspěšného pokusu apod.

Rapid Release aktualizace

Tyto aktualizace se dají stahovat pomocí utility LiveUpdate, nebo skripty, které jsou dodávány výrobcem. Rapid Release definice velmi rychle reagují na objevení škodlivého kódu, kdy jeho signatura je v řádu minut zapracována do balíku aktualizací a umístěna na distribuční zdroje ke stažení. Tyto definice se využívají v době hlášených virových záplav a procházení omezenou sadou kontrol oproti neškodnému kódu.

Aktualizace pomocí spustitelného souboru

Výrobce poskytuje aktualizace i ve spustitelném souboru, a to .exe a .jdb. Aktualizace produktů probíhá jejich automatickým stažením pomocí skriptu nebo manuálním stažením, kdy je soubor nakopírován do definovaných adresářů opět automaticky nebo manuálně. Následně dojde k jeho automatickému spuštění a aktualizaci produktu.

Podmínky pro úspěšnou distribuci virových řetězců a provozování aktualizačních mechanismů

Dostupný jeden zdroj aktualizací v Internetu – webové sídlo výrobce. Tento zdroj nemusí být dostupný ze všech používaných produktů nebo klientů. Minimálně však musí tento zdroj mít dostupný SEP manager.

Povolené komunikační porty na Interní nebo externí aktualizační zdroj (HTTP(s) nebo FTP protokol).

Preferovaný systém aktualizací

Preferovaným systémem aktualizací je využívat metodu LiveUpdate k získávání certifikovaných aktualizací a využít možnosti hierarchické distribuce definic na koncové body následovně:

- Aktualizace serverových aplikací SEP Policy Manager.
- Podle typu destinace použít buď aktualizační zdroj Group Update Provider nebo využít přímé konektivity klientů na SEP Policy Managery.

Využití Rapid Release definic doporučujeme jen v případech varování před virovou záplavou na produktech instalovaných na perimetru sítě.

Manuální aktualizace doporučujeme provádět jen na koncových klientech a to pouze v případech, kdy ostatní metody selžou, nebo je toto doporučeno výrobcem.

Pro přehlednost jsou v následující tabulce uvedeny navrhované pravidelné časy stahování aktualizací pro jednotlivé produkty:

Produkt	Četnost ověřování antivirových a antispamových definic
Symantec Endpoint Protection 12.1	4 hodiny na SEP Policy Manager (SEP Policy Manager posílá okamžitě automaticky definice svým klientům).

Časy jsou navrženy na základě doporučení výrobce a na základě dlouhodobé zkušenosti s produkty.

1.2.2. MOŽNOSTI ROZŠIŘOVÁNÍ O DALŠÍ VERZE A PRVKY ANTIVIROVÉ, ANTISPAMOVÉ KONTROLY

Jsou dvě možnosti, jak doplnit navrhovanou antivirovou ochranu:

- Implementace dalších funkcionalit.
- Implementace dalších nových produktů.

Implementace dalších funkcionalit navrhovaných produktů

Symantec Endpoint Protection 12.1

Využití nepoužívaných funkcionalit Produktu SEP 12.1 pro vyšší zabezpečení prostředí proti vniknutí a šíření škodlivých kódů, konkrétně nasazení těchto funkcionalit:

- Kontrola aplikací a zařízení.

Tyto funkcionality SEP 12.1 jsou nedílnou součástí nabízených licencí a výrazně umožňují zvýšit bezpečnost prostředí.

1.2.3. MOŽNOSTI A PODMÍNKY CENTRÁLNÍ SPRAVY SYSTÉMU

Všechny jednotlivé nabízené produkty mají svoji administrátorskou konzolu, která zajišťuje tyto funkce:

- Instalace koncových balíčků (SEP 12.1).
- Management a deployment politik ochrany a aktualizací.

Vyrozumívání systému ve formě:

- Stavových dat.
- Alertů.
- Reportů.
- Log záznamů.

Blíže centrální správu u jednotlivých produktů charakterizuje následující tabulka:

Produkt	Typ konzoly	Funkce konzoly
Symantec Endpoint Protection 12.1	Java konzola, Web konzola	Konfigurace politik ochrany a aktualizací. Nastavování alertů a notifikací. Instalace a upgrade klientů, vytváření struktury skupin pro klienty, přesunování klientů mezi skupinami Zobrazování stavových dat, log záznamů, zobrazování reportů, zasílání reportů.

Nastavení oprávnění pro antivirovou ochranu serverů, stanic a notebooků

Produkt Symantec Endpoint Protection 12.1 umožňuje nastavení oprávnění ve třech úrovních, tak navrhujeme definovat oprávnění následovně:

Úroveň oprávnění	Popis oprávnění	
L1 oprávnění	Plná oprávnění nad celou Site	Servisní organizace
L2 oprávnění	Administrátorská oprávnění pro jednotlivé celky	

Úroveň oprávnění	Popis oprávnění	
L3 oprávnění	Omezená oprávnění pro celky s možností vidět reporty, alerty, logy, není možno nastavovat politiky	

Nastavení oprávnění pro antivirovou ochranu

Administrátorský účet	Oprávnění
MCOM	Plná oprávnění – servisní organizace.
	Omezená oprávnění – standardní uživatelský účet s oprávněním spouštět speciální úlohy: • Restart/shutdown serverů • Restart procesů

Nastavení oprávnění na operačních systémech serverů

Administrátorský účet	Oprávnění
MCOM	Plná oprávnění – servisní organizace.
	Omezená oprávnění – standardní uživatelský účet s oprávněním spouštět speciální úlohy: • Restart/shutdown serverů • Restart procesů

Podmínky úspěšného provozu centrální správy

Technické podmínky

Dostupné konzoly na definovaných portech – nastavení prostupů na firewallu a dalších prvcích KI.

Vzdálený přístup k management rozhraní SEP serveru pro monitoring, dohled a vyhodnocení.

Provozní a procesní podmínky

Administrátorské a operátorské role v jednotlivých produktech.

Zaškolení správců – před přidělením oprávnění je nezbytné administrátory a operátory proškolit v oblasti administrace navrhovaných produktů.

Harmonogram implementačních prací

Instalace SEPM s interní databází, exporty instalačních balíčků, záloha konfigurace, nastavení zálohování	2 dny
Konfigurace politik a notifikaci, reportů, GUP	2 dny
Zaškolení	1 den

1. HW A SW POŽADAVKY PRO IMPLEMENTACE

OS Windows 2008 R2 EN STD
4 CPU
6 GB RAM
60 GB Systém
100 GB Data
100 GB Backup
Ethernet interface s dostupnou propustností až 1 Gb/s

2. ROZSAH IPLEMENTAČNÍCH PRACÍ

- 1x instalace a implementace Symantec Endpoint Protection Manager včetně interní databáze, kde následně bude provedena záloha konfigurace a nastavení zálohování.

- Konfigurace management rozhraní a to zejména přístupové účty, práva, stahování a distribuce definic a update, vytvoření skupin, politiky pro AV, FW, IDS/IPS, konfigurace plánovaných scanů, reporty, notifikace, vytvoření instalačních balíčků

3. KONFIGURACE A PODMÍNKY IPLEMNETAČNÍ KONFIGURACE

Požadovaná konfigurace management serveru před započetím implementace Symantec Endpoint Protection :

1. Vytvořený virtuální server s OS Windows 2008 R2 STD s realizovanými aktualizacemi a HW parametry viz. bod 2

Upřesnění rozsahu konfiguračních prací v rámci implementace:
Do management rozhraní budou nastaveny přístupy pro Administrátory a Operátory, které se liší úrovní oprávnění do maximálního počtu 4 uživatelů.

Dále v management rozhraní budou vytvořeny instalační balíčky dle požadavků administrátora a vyexportovány pro použití na instalaci koncových bodů do maximálního počtu 4.
Nastavení dvou vzorových „Location" pro změny chování chráněného koncového bodu například uvnitř sítě a mimo interní síť.

Vzorová instalace koncového bodu a to pomocí dvou metod:
a, vzdáleně prostřednictvím management rozhraní
b, lokálně na koncovém bodu pomocí instalačního balíčku.
Maximálně však šest instalovaných koncových bodů.

Konfigurace funkcionality antivirového klienta Group Update Provider – jakýkoliv z koncových bodů provozovaných ve vzdálené lokalitě a určený pro lokální distribuci definic na vzdálené lokalitě. Nejedná se o implementaci dalšího modulu, pouze o konfiguraci základní funkcionality každého koncového bodu, která umožňuje libovolnému koncovému bodu stát se distribučním bodem pro distribuci definic ostatním klientům v dané lokalitě a efektivně tak snížit zatížení komunikačních linek LAN, WAN, MAN při distribuci aktualizací v rámci rozsáhlých sítí. Maximální počet jeden.

Dále budou v rámci implementace nastaveny požadované reporty a notifikace.

Při implementaci budou zároveň vytvořeny skupiny koncových bodů (klientů), na které bude následně možno zacílit jednotlivá pravidla chování všech funkcionalit dodávaného řešení. V rámci našich zkušeností doporučujeme vytvořit následující skupiny:

- **Servers** – skupina pro servery, kde nebude instalován firewall a application and device control
- **Computers** – pevné počítače s nainstalovaným plným balíkem zabezpečení
- **Computers Admin** – pevné počítače s nainstalovaným plným balíkem zabezpečení s možností úpravy firewallu
- **Notebooks** - notebooky s nainstalovaným plným balíkem zabezpečení
- **Notebooks Admin** - notebooky s nainstalovaným plným balíkem zabezpečení s možností úpravy firewallu

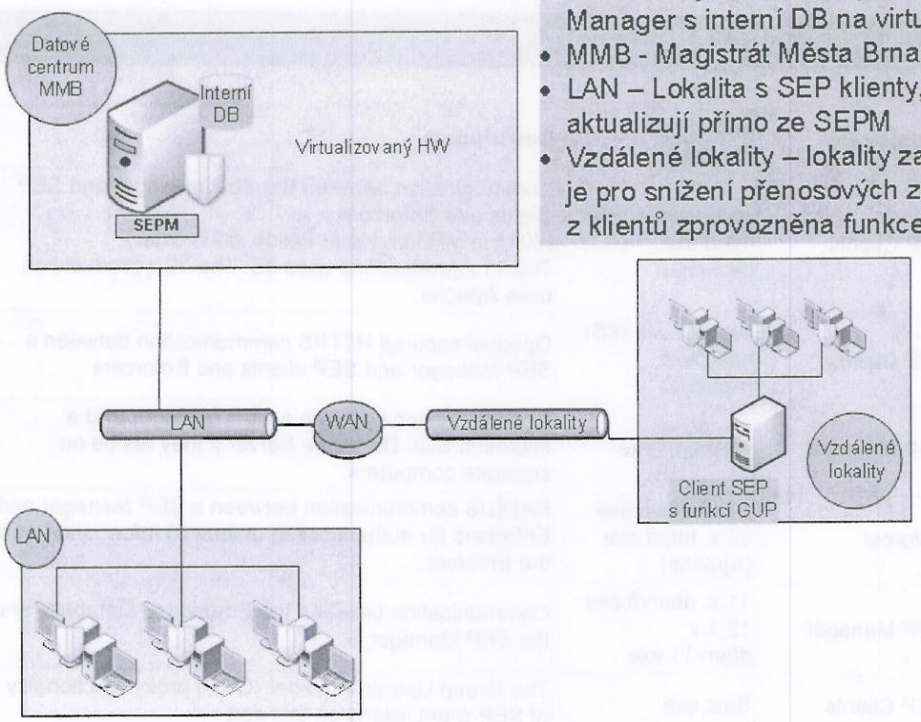
  Maximální počet tvořených skupin v rámci implementace je pět.

4. KOMUNIKAČNÍ PORTY NAVRHOVANÉHO ŘEŠENÍ

Port Number	Port Type	Initiated By	Listening Process	Description
80, 8014	TCP	SEP Clients	svchost.exe (IIS) httpd.exe (Apache)	Communication between the SEP manager and SEP clients and Enforcers. (8014 in MR3 and later builds, 80 in older). The 11.x product line uses IIS. The 12.x product line uses Apache.
443	TCP	SEP Clients	svchost.exe (IIS) httpd.exe (Apache)	Optional secured HTTPS communication between a SEP Manager and SEP clients and Enforcers.
1433	TCP	SEP Manager	sqlserver.exe	Communication between a SEP Manager and a Microsoft SQL Database Server if they reside on separate computers.
1812	UDP	Enforcer	11.x: w3wp.exe 12.x: httpd.exe (Apache)	RADIUS communication between a SEP Manager and Enforcers for authenticating unique ID information with the Enforcer.
2638	TCP	SEP Manager	11.x: dbsrv9.exe 12.1.x: dbsrv11.exe	Communication between the Embedded Database and the SEP Manager.
2967	TCP	SEP Clients	Smc.exe	The Group Update Provider (GUP) proxy functionality of SEP client listens on this port.
8005/8765	TCP	SEP Manager	SemSvc.exe	This is the Tomcat Shutdown port. In the 11.x product line SEP Manager listens on the Tomcat default port of 8005 except RU7 uses 8765. Also in 12.x product line port 8765 is used instead.
8045	TCP	SEP Manager	SemSvc.exe	In the SEP 11 RU6 SEPM, the registry is started by the Tomcat servlet container. CreamTec's AjaxSwing uses the existing registry to communicate with its client agents that run in stand alone mode
8443	TCP	Remote Java or Web Console	SemSvc.exe	HTTPS communication between a remote management console and the SEP Manager. All login information and administrative communication takes place using this secure port.
8444	TCP	Symantec Protection Center	SemSvc.exe	This is the SEPM web services port. SPC 2.X makes Data Feed and Workflow requests to SEPM over this

		v 2.X		port.
8445	TCP	Reporting Console	httpd.exe (Apache)	Added in 12.1.x. HTTPS reporting console
9090	TCP	Remote Web Console	SemSvc.exe	Initial HTTP communication between a remote management console and the SEP Manager (to display the login screen only).
39999	UDP	Enforcer	SNAC.exe (Windows SNAC) CClientCtl.exe (Windows ODC) SNAC (Mac SNAC/ODC)	Communication between the SEP Cients and the Enforcer. This is used to authenticate Clients by the Enforcer.

5. NÁVRH SCHÉMATU INFRASTRUKTÚRY



Vysvětlivky ke schématu

- SEPM – Symantec Endpoint Protection Manager s interní DB na virtualizovaném HW
- MMB - Magistrát Města Brna
- LAN – Lokalita s SEP klienty, kteří se aktualizují přímo ze SEPM
- Vzdálené lokality – lokality za WAN/MAN, kde je pro snížení přenosových zátěží na některém z klientů zprovozněna funkce GUP