FAKULTNÍ NEMOCNICE BRNO

FAKULTNÍ NEMOCNICE BRNO

držitel akreditace DIAS a certifikace ISO 9001

Jihlavská 20, 625 00 Brno
IČO 652 69 705

ODBOR OBCHODU A MARKETINGU / OBCHODNÍ ODDĚLENÍ

Sekretariát:
Tel.:532 232 001

Naše zn.: 2016/../FNBRNO – 15.2.2 – Va/Eg
Vaše zn.: -

V Brně dne 21. prosince 2016

Žádost o podání nabídky k veřejné zakázce malého rozsahu

1. Vymezení předmětu plnění

Předmětem plnění je zajištění komplexní ochrany serverů a koncových stanic včetně podpory pořízeného řešení na dobu 3 let. Zadavatel řešením zabezpečí ochranu provozovaných systémů na platformě MS Windows a Linux, včetně antispamové ochrany jak pro tradiční, tak pro virtualizovanou infrastrukturu FN Brno dle technické specifikace uvedené v příloze č. 1 této výzvy.

Popis současného stavu

Zadavatel provozuje 24 ESXi serverů a 250 serverů ve virtuálním režimu na platformě VMware vSphere 6.5. V současné době provozuje zadavatel také 1200 virtuálních desktopů na platformě VMware Horizon 7 a 1000 mobilních zařízení s operačním systémem Android 4.4 a vyšším. Operačním systémem serverů jsou produkty společnosti Microsoft ve verzích Windows 2008 až 2012 R2 Server respektive mutace Linux. Používaným poštovním systémem je MS Exchange 2013. Portálové služby jsou zabezpečovány MS SharePoint 2013 Serverem. Koncové stanice jsou zadavatelem provozovány s operačními systémy MS Windows XP, W7 a W10 (architektura x86 a x64).
Zadavatel využívá pro zabezpečení antivirové ochrany produkt Trend Micro. Pro zajištění antispamové ochrany na perimetru je využíván produkt Trend Micro.

2. Místo a termín plnění

- Místem plnění je Fakultní nemocnice Brno, Pracoviště medicíny dospělého věku, Centrum informatiky, Jihlavská 20, 625 00 Brno
- Termín plnění 3 roky. Zadavatel požaduje začít plnění neprodleně po uzavření smlouvy.

3. Podmínky pro plnění

Nabídka bude zpracována v českém jazyce a předložena v jednom originále v písemné formě v listinné podobě a bude vložena do obálky označené slovy „Nabídka – **Antivirové řešení pro FN Brno** - Neotevírat“.

Nabídka bude obsahovat:

- obsah nabídky – seznam předkládaných dokumentů,
- krycí list zájemce obsahující identifikační údaje uchazeče, a to obchodní firmu nebo název, sídlo, právní formu, IČ, DIČ, bankovní spojení, statutární orgán, telefonní, faxové a e-mailové spojení, adresu pro doručování písemností, internetovou adresu apod.,
- cenovou nabídku dle 4. bodu této výzvy s technickou specifikací v českém jazyce,

- návrh smlouvy podepsaný osobou oprávněnou jednat jménem zájemce nebo za zájemce.

Nabídka bude zabezpečena takovým způsobem, který znemožní vyjmout jednotlivé listy nabídky. Opatření proti vyjmutí listů, uplatňuje zadavatel zejména z důvodů vyloučení možnosti neoprávněné manipulace. Jednotlivé listy nabídky budou číslovány nepřetržitou číselnou řadou. Jako poslední list nabídky bude doloženo prohlášení uchazeče, podepsané statutárním zástupcem uchazeče, o počtu stran nabídky.

4. Požadavky na způsob zpracování nabídkové ceny a platební podmínky

Celková nabídková cena bude zpracována v Kč bez DPH, včetně DPH, s vyčíslením DPH zvlášť a s uvedením sazby DPH, a bude zahrnovat veškeré náklady spojené s dodávkou předmětu plnění, tj. zejména dopravu zboží do místa dodání, obaly, naložení, složení, pojištění během dopravy, případné clo, instalaci, uvedení do provozu, provedení funkční zkoušky, recyklační poplatek (pouze u zboží, které tomuto poplatku podle zákona č. 185/2001 Sb., o odpadech, ve znění pozdějších předpisů, podléhá).

Cena bude stanovena jako maximální a nepřekročitelná a její změna bude možná jen v případě legislativních změn, které mají prokazatelný vliv na výši nabídkové ceny.

Platební podmínky: Fakturu - daňový doklad vystaví prodávající po splnění dodávky a předání předmětu plnění kupujícímu. Splatnost faktury je rozložena do 8 rovnoměrných splátek, první splátka 60 dnů od data vystavení faktury, každá další splátka 30 dnů od splatnosti předchozí splátky. Součástí faktury bude splátkový kalendář, datum splatnosti faktury bude shodné s datem poslední splátky. Datum uskutečnění zdanitelného plnění bude shodné s datem předání předmětu plnění kupujícímu, tj. datem podpisu předávacího protokolu.

5. Způsob hodnocení nabídek

Nabídka bude hodnocena podle základního hodnotícího kritéria, kterým je nejnižší nabídková cena bez DPH.

6. Poskytování dodatečných informací

V případě, že některý z dodavatelů bude mít jakýkoliv dotaz vztahující se k zadávacím podmínkám veřejné zakázky, musí tento dotaz podat prostřednictvím profilu zadavatele, jímž je elektronický nástroj E-ZAK. Žádost o dodatečnou informaci k zadávacím podmínkám je dodavatel povinen doručit zadavateli nejpozději 5 pracovních dnů před uplynutím lhůty pro podání nabídek. Zadavatel odešle dodavateli odpověď na jeho žádost nejpozději do 11:00 hodin posledního pracovního dne předcházejícího poslednímu dni lhůty pro podání nabídek. Zadavatel může poskytnout dodavatelům dodatečné informace k zadávacím podmínkám i bez předchozí žádosti. Dodatečné informace, včetně přesného znění případné žádosti, poskytne zadavatel hromadně i všem ostatním dodavatelům prostřednictvím svého profilu (https://ezak.fnbrno.cz/).

7. Zadavatel si vyhrazuje právo

Zadavatel si vyhrazuje právo řízení na veřejnou zakázku zrušit (z jakéhokoliv důvodu) až do okamžiku uzavření smlouvy s vybraným uchazečem.

8. Lhůta a místo podání nabídky

Lhůta:
- lhůta pro podání nabídky se stanovuje do **9. 1. 2017 do 11,00 hod.**

Místo:
- poštou doporučeně na adresu:

Fakultní nemocnice Brno
Odbor obchodu a marketingu - Obchodní oddělení
Jihlavská 20
625 00 Brno

- osobně na výše uvedené adrese pavilon P, Odbor obchodu a marketingu – Obchodní oddělení, přízemí, dveře č. 1070 v pracovních dnech od 8,00 do 11,00 hod.

9. Název a sídlo organizace

Fakultní nemocnice Brno, Jihlavská 20, 625 00 Brno

Ing. Lenka Vamberská
vedoucí obchodního oddělení

Přílohy:
Příloha č. 1 - Technická specifikace

Vyřizuje: Ing. Hana Egerlová, tel. 532 784

Signature Not Verified
Digitally signed by Ing. Lenka Vamberská
Date: 2016.12.21 13:51:26 +01:00
Reason:
Location:

Příloha č. 1

Technická specifikace

Zadavatel upozorňuje, že v případě číselně vyjádřených technických parametrů je možné se od nich odchýlit o +/- 10%, pokud to jejich povaha umožňuje a za podmínky splnění požadovaného účelu. U obecných požadavků na elektrickou bezpečnost a napájení a dalších požadavků, u nichž je tak výslovně uvedeno, se odchýlit nelze.

Technická specifikace:

I. Ochrana tradičních koncových stanic:

- Antivirovou a antimalware ochranu 3000 tradičních (železných) koncových stanic (MS Windows XP, W7, W8, W10).
- Detekci a blokování hrozeb v reálném čase.
- Prohledávaní hrozeb na stanici na vyžádání nebo v nastaveném čase.
- Prohledávání hrozeb na stanici při nečinnosti stanice (zámek obrazovky, spořič obrazovky).
- Funkcionalitu „tiché“ vzdálené instalace na koncové stanice včetně bezobslužné konfigurace.
- Ochranu před síťovými hrozbami – ochrana prohlížeče, ochrana před přístupem na škodlivé weby, botnet ochrana a ochrana před vzdáleným napadnutím.
- Host-based Intrusion Prevention (HIPS).
- Systém IPS musí podrobně zjistit zranitelnosti systémů a aplikací na vyžádání nebo automaticky dle CVE (Common Vulnerabilities and Exposures) skóre aplikovat relevantní ochranu.
- Aktivní ochranu před neznámými hrozbami (zero hour/zero day).
- Funkcionalitu politikou řízených povolených/zakázaných aplikací.
- Ochranu před logováním kláves a přetečení zásobníku.
- Funkcionalitu blokace USB portů (výměnných zařízení).
- Logování operací s výměnnými zařízeními.
- Zamezení používání neschválené třídy zařízení nebo konkrétního zařízení, např. konkrétního výrobce – rozeznávání Class i Device ID.
- Centrální konzoli pro správu ochranného systému, která umožňuje synchronizaci s Active Directory FN Brno.
- Server centrální správy musí být možné nainstalovat na Windows, Linux a virtuální appliance.

II. Ochrana serverů a virtualizované infrastruktury

- Antivirovou a antimalware ochranu 10 tradičních (železných) serverů (s OS MS Windows /Linux).
- Antivirovou a antimalware ochranu virtuálních serverů v režimu bez agentů založenou na technologii VMware vSafe API pro 12 ks ESXi – 24 CPU soketů (nebo 300 serverů).
- Antivirovou a antimalware ochranu virtuálních desktopů v režimu bez agentů založenou na technologii VMware vSafe API pro 12 ks ESXi – 24 CPU soketů (nebo 1200 desktopů).
- Pro zabezpečení antivirové ochrany virtualizovaných serverů a koncových stanic požaduje zadavatel použít model licencování ve variantě – licence na počet ESX serverů (celkem 24 ks ESXi – 48 CPU Soketů).
- Systém musí umožňovat real-time a on-demand ochranu.
- Systém musí umožňovat cache mechanismus pro všechny chráněné servery pro snížení dopadu na výkon skenovaných systémů.
- IPS a firewall ochranu 10 tradičních (železných) serverů (s OS MS Windows / Linux).
- Ochranu před síťovými hrozbami – ochranu před komunikaci se škodlivými destinacemi a ochranu před vzdáleným napadnutím serverových služeb – sledování zranitelností systému.
- Systém IPS tradičních serverů a koncových stanic musí podrobně zjistit zranitelnosti systémů a aplikací na vyžádání nebo automaticky, popsat je dle CVE skóre a aplikovat automaticky relevantní ochranu.

- Centrální konzola propojená s Active Directory FN Brno a VMware vCenter, tak aby byla zajištěna okamžitá automatizovaná ochrana nových virtuálních a fyzických instancí, přesouvaných instancí přes VMware vMotion a spících instancí.

III. Ochrana emailových systémů

- Antivirovou ochranu 3 serverů IBM Domino.
- Antispamovou ochranu 3 ks serverů IBM Lotus Notes (instalovaných na MS Windows 2012 R2) s napojením na systém globálních reputací s možností tvorby White Listů.
- Antispamovou ochranu 3 ks serverů MS Exchange 2013 s napojením na systém globálních reputací s možností tvorby White Listů.
- Společná ochrana celého serveru, schránek i serverové části.
- Antivirus a antispyware.
- Antispam s funkcí graylisting.
- Detekce typu souborů v reálném čase.
- Možnost správy přes příkazovou řádku.
- Sledování výkonu serveru v reálném čase.
- Možnosti pro nastavení pravidel inspekce souborů – mazání spustitelných souborů, skriptů.

V. Ochrana mobilních zařízení

- Antivirovou ochranu podporující aktuální verzi Android.

Pokročilé funkce:

- Anti-Theft – při ztrátě mobilu ochrání SMS, fotky, e-maily a soukromí.
- Karanténa – viry a hrozby jsou okamžitě vymazány nebo uloženy do karantény s možností obnovy souborů.
- Bezpečnostní audit – sleduje funkce zařízení (stav baterie, volné místo na disku, spuštěné procesy, Bluetooth, infračervený port, viditelnost zařízení). Po zjištění nedostatků nabídne řešení.
- Ochrana heslem – ochrana programu před změnou nastavení Anti-Theft a odinstalováním.
- Pokročilá heuristická analýza – chrání vás před neznámými hrozbami.

Ochrana před zneužitím:

- Ochrání před krádeží nebo zneužitím mobilu.
- Mazání na dálku – zasláním SMS odstraníte všechny osobní informace včetně kontaktů, zpráv a obsahu datových karet.
- Kontrola SIM – při vložení neznámé SIM karty se automaticky odešle na určené mobilní číslo zpráva s telefonním číslem vložené karty, její IMSI a IMEI.

VI. Ochrana SharePoint serveru

- Ochrana celého serveru včetně rezidentního štítu
- Skenování databází
- Filtrování na základě definovatelných pravidel
- Automatická detekce a zařazení kritických souborů do výjimek s možnost tvorby vlastních výjimek

IV. Implementace a podpora systému ochrany

Implementace v rozsahu:

- Instalace a integrace centrální konzoly
- Vzdálená bezobslužná instalace agentů (založená na distribuci politik přes centrální konzoli) na vybrané koncové systémy (10 VD)
- Vzdálená bezobslužná instalace agentů (založená na distribuci politik přes centrální konzoly) na vybrané koncové systémy (10 PC)
- Instalace emailové ochrany (1 server)
- Zaškolení 2 pracovníků zadavatele v rozsahu každého alespoň 8 hodin.
- Systém antimalware ochrany musí mít v posledním 1 roce vynikajícími výsledky z nezávislých testů.

- Zadavatel požaduje popis (návod) instalace antivirového systému v českém jazyce.
- Zadavatel požaduje instalaci na 5 endpointů (virtuálních serverů) vybraných zadavatelem s předvedením funkcionality řešení před podpisem smlouvy (Systém ochrany pro koncové stanice, serverů a emailu musí mít minimální dopad na výkon chráněného aktiva a síť).
- Podporu na úrovni aktualizace virových a antispamových definic po dobu **3** let.

Místo a termín plnění

- Místem plnění je FN Brno, PMDV, CI, Jihlavská 20, 625 00 Brno
- Termín plnění **3** roky. Zadavatel požaduje začít plnění neprodleně po uzavření smlouvy.