### Příloha č. 10 Zadávací dokumentace – změna č. 1 ze dne 19.07.2019

## Specifikace předmětu část 4 - Dodávka technologií a HW vybavení pro zajištění bezpečnosti a provoz centralizovaného řešení

Předmětem plnění je zavedení:

* monitorovacího systému
* monitoringu sítě (datové toky, anomálie, sběr a vyhodnocení), centrální logovací nástroje
* dodávka serverového operačního systému
* dodávka licenci
* implementace

Součástí dodávky je záruka na dobu udržitelnosti, tj. 5 let. Zadavatel u HW předpokládá standardní záruku u zboží v délce 3 let a její prodloužení na dobu 5 let uchazeč promítne do ceny technické podpory.

### Bezpečnost

#### Monitorovací systém

Předmětem plnění je dodávka provozního monitorovacího systému, který umožni online dohled provozních a serverových služeb a zařízení. Systém monitoruje dění v celém rozsahu poskytovaných služeb. Současně poskytuje notifikace o zjištěných anomáliích formou emailu.

*Tabulka č. 1 – požadované vlastnosti monitorovacího systému*

|  |  |
| --- | --- |
| Název | Splněno |
| Monitorovací systém pro vyhodnocení systémových služeb v režimu 24x7 | ANO/NE |
| Přehledné webové prostředí | ANO/NE |
| Ukládání dat do databáze, archivace logů min 1 rok | ANO/NE |
| Webový nástroj - konzole pro správu a snadnou konfiguraci senzorů | ANO/NE |
| Přehledný konfigurovatelný panel (Dashboard) na úvodní stránce se živými grafy | ANO/NE |
| Sledování základních parametrů sítě a síťových služeb pomocí senzorů | ANO/NE |
| Systém obsahuje min. 100 typů různých senzorů pro sledování stavu služeb | ANO/NE |
| Podpora protokolů SNMP (všechny současné verze), WMI monitoring | ANO/NE |
| Analytické nástroje pro přehledné vyhodnocování aktuálních i historických stavů | ANO/NE |
| Vyhodnocování provozních statistik formou přehledných grafů – live data, historická data, SLA | ANO/NE |
| Možnost vložit mapu sítě | ANO/NE |
| Možnost definice alarmů, možnost jejich editace a nastavení | ANO/NE |
| Podpora monitoringu SNMP, WMI, plovoucí monitoring, packet sniffing, IPv4 a IPv6 | ANO/NE |
| Podpora operačních systémů Windows, Linux, Mac OS | ANO/NE |
| Software bude instalován v prostředí technologického centra zadavatele | ANO/NE |
| Forma klienta Webová konzole | ANO/NE |
| Klient dostupný i pro mobilní platformu Apple a Android | ANO/NE |
| Agent pro MSSQL server, Linux, Exchange server, Vmware | ANO/NE |
| Součástí dodávky je licence provozovaného operačního systému | ANO/NE |
| V licenci zahrnuto min. 1000 senzorů | ANO/NE |
| Součástí dodávky je nastavení monitorovacího systému pro technologické prostředí a zaškolení Administrátorů | ANO/NE |
| Technická podpora po dobu 5 let | ANO/NE |
| Název a popis dodávaného nástroje, odkaz na katalogový list  Doplní dodavatel |  |

#### Monitoring sítě a centrální logovací nástroj

Předmětem plnění je dodávka síťové monitorovací technologie a sběru logů ze síťových prvků a infrastruktury.

Monitoring sítě je sonda, která poskytuje obraz provozu uvnitř sítě, který je nezbytnou součástí v boji proti kybernetickým hrozbám vč. těch uvnitř sítě (např. ransomware). Rozšíření o automatickou detekci anomálií zajistí kontrolu drobného provozu a včasnou notifikaci v případech, kdy se mění chování jednotlivých uzlů v síti, které je zásadně odlišné předchozímu. Zároveň upozorní na nežádoucí komunikace, které mohou vynášet informace nebo jinak škodit. Je vhodným doplněním pro komplexní monitoring síťového dění vč. trendů a statistik chování. Účinně tak doplní provozní monitoring i ochranu perimetru, tj. firewall. Sonda bude umístěna na centrálním prvku a bude monitorovat veškerý provoz vnitřní i vnější sítě.

Centrální logovací nástroj - centrální místo pro uchování/archivaci a normalizace veškerých provozních logů na jednom místě s jednou konzolou s vizualizacemi, trendy a zejména nástrojem full-textového vyhledávání napříč celou bází zaznamenaných informací. Integrace logů na jednom místě spolu s jejich dlouhodobým uchováním je základem nejen pro forenzní analýzy, ale spolu s celou řadou integrovaných parserů dokáže poskytovat konkrétní upozornění a progresivní reporting z oblasti bezpečnosti ale i provozu

*Tabulka č. 2 – požadované vlastnosti monitorovacího systému sítě a logovacího nástroje*

|  |  |
| --- | --- |
| Název | Splněno |
| Systém poskytující statistiky o sítové komunikaci ve formě IP toku (NetFlow v5/v9, IPFIX) | ANO/NE |
| Vestavěný kolektor pro uchování a analýzu statistik o síťovém provozu z vrstev L2-L4 a L7. | ANO/NE |
| Jednoduché nasazení a intuitivní GUI. Sondu lze umístit do libovolného bodu v síti.  Intuitivní nasazení konfigurace které umožňuje plně automatické NetFlow monitorovací řešení během několika minut. | ANO/NE |
| Rychlá a automatická a detekce vážných bezpečnostních událostí v raných fázích útoku jako jsou neznámý malware, RAT (remote access trojan), command and control, úniky dat, či další pokročilé, persistentní a cílené hrozby | ANO/NE |
| Detekce výkonnostní anomálie a chybné konfigurace zařízení.  Toto umožňuje preventivně reagovat, a zabránit tak tomu, aby tyto problémy v budoucnu způsobily výpadky sítě a služeb nebo nějaká jiná ohrožení. | ANO/NE |
| Interaktivní dashboard poskytuje celkový přehled o stavu datové sítě s možností získat okamžitě ke každé události | ANO/NE |
| Podpora behaviorální analýzy, která umožňuje odhalovat dosud neznámé nebo specifické hrozby, pro které signatura neexistuje | ANO/NE |
| Detailní informace o provozu, který danou událost způsobil.  Rychlé vyšetřování a řešení problémů – systém nahrává metadata o síťovém provozu z posledních min. 6 měsíců, která poskytnout rychlé a detailní informace o příčinách a povaze problémů. Tato data je možno libovolně zobrazovat, třídit a filtrovat. | ANO/NE |
| Rychlé nasazení produktu, nevyžaduje zdlouhavé nastavování a ladění řady monitorovaných parametrů.  Umělá inteligence a strojové učení detekuje automaticky provozní a výkonnostní anomálie v reálném čase. Pomocí systému lze sledovat výkonnostní parametry až do jednotlivých transakcí uživatelů (např. SQL dotazy). | ANO/NE |
| Viditelnost do dění v síti – cílem je získat celkový přehled i detailní a hluboký vhled do dění v síti a hrozbách a rizicích, které se zde vyskytují – ve všech podsítích, všech zařízeních a všech aktivních službách na každém zařízení. | ANO/NE |
| Přehled o všech zařízeních, které se připojují k firemní síti, včetně toho jaké služby využívají, s kým komunikují, jaký typ komunikace atd | ANO/NE |
| Systém dokáže detekovat porušení bezpečnostních politik a souladu s nařízeními, které se týkají používání zranitelných a zastaralých verzí systémových nástrojů, nešifrovaných hesel, stahování modifikovaných multimediálních souborů a dokumentů, skutečné úrovně šifrování (HTTPS), přístupů k externím a interním zdrojům, používání mobilních zařízení atd. | ANO/NE |
| Uchování kompletních informací o síťovém provozu po dobu min 6 měsíců. | ANO/NE |
| Forma dodávky – samostatná appliance vhodná pro montáž do 19“ rozvaděče | ANO/NE |
| Licence pro 1 sondu s napojením na síťový cluster | ANO/NE |
| Periodické vyhodnocování statistik a rozbor hrozeb formou služby 1x za 6 měsíců formou předplacené technické podpory | ANO/NE |
| Dodávka do sídla zadavatele, zapojení do síťového prostředí, nastavení monitorovacích pravidel a zaškolení Administrátorů systému | ANO/NE |
| Technická dokumentace nastavení | ANO/NE |
| Technická podpora po dobu 5 let formou opravy / výměny do následujícího dne | ANO/NE |
| Název a popis dodávaného nástroje, odkaz na katalogový list  Doplní dodavatel |  |

### Server včetně operačního systému

Předmětem je dodávka vhodného server pro provoz virtuálních strojů, kompatibilního se stávajícím prostředím – viz Příloha č. 6 – Popis stávajícího stavu. Dále je předmětem dodávka 64 bit operačního systému.

**Server – 1ks**

*Tabulka č. 3 – požadované technické parametry dodávky serveru*

|  |  |
| --- | --- |
| Název | Splněno |
| 2U rackmount provedení | ANO/NE |
| 64 bitová architektura kompatibilní se stávajícím HW vybavením na úrovni architektury a virtualizace umožňující vysokou dostupnost  Minimálně 2x 8core procesor L3 cache alespoň 20MB, podpora DDR4 ECC min., procesor musí umožnit vypnutí nevytížených jader kvůli úspoře elektrické energie | ANO/NE |
| serverový systém s minimálním výkonem podle benchmark <http://www.spec.org/cpu2017/results/>  SPECrate2017\_int = 78 | ANO/NE |
| paměť min. 128 GB rozšiřitelná min. na 256GB typu DDR4 | ANO/NE |
| Osazeno 3ks interní 2,5“ disky hot-plug disky min. 500GB/10k/SAS nebo SSD v konfiguraci RAID5 s rychlostí min. 6Gbit/s. | ANO/NE |
| samostatný RAID řadič s podporou RAID 1,0,1+0,5,6, cache min 1024MB bateriově  zálohovaná, cache funkce - Writeback, Write-through, AdaptiveReadAhead, Non-ReadAhead, ReadAhead | ANO/NE |
| Dvouportová (nebo dvě jednoportové) 8Gbps FibreChannel HBA. | ANO/NE |
| Síťové připojení – min. 6 portů s min. rychlostí 1Gbit/s , min. 4x samostatný NIC na MB, | ANO/NE |
| podpora TOE a SCSI Offload, WOL, SCSI boot, IPv4, IPv6, podpora Jumbo frame (802.3ab) u všech 1Gbit/s Ethernet portů | ANO/NE |
| Interní DVD-ROM mechanika | ANO/NE |
| Min.: 4x externí USB 2.0 port | ANO/NE |
| Redundantní napájení a chlazení | ANO/NE |
| podpora řízení napájení serverů provozovanou serverovou virtualizaci vmware 6.5 | ANO/NE |
| Management a vzdálená konzole přístupu na server | ANO/NE |
| Interní port pro USB klíč, nebo interní slot pro SD kartu, s podporou bootování | ANO/NE |
| Umístění na ližinách umožňující vysunutí serveru se zapojenou kabeláží. Ližiny jsou součástí dodávky | ANO/NE |
| Server uveden na listu kompatibility pro nabízenou serverovou virtualizaci a kompatibilní se stávajícím vybavením úřadu. | ANO/NE |
| Záruka 5 let formou opravy / výměny do následujícího dne | ANO/NE |
| Název a popis dodávaného zboží, odkaz na katalogový list  Doplní dodavatel |  |

**Operační systém – 1ks**

*Tabulka č. 4 – požadované technické parametry dodávky operačního systému*

|  |  |
| --- | --- |
| Název | Splněno |
| 64 bit operační systém kompatibilní s Microsoft Active Directory | ANO/NE |
| Kompatibilní s provozovanými aplikacemi ve virtuálním prostředí a dodaným virtualizačním řešením | ANO/NE |
| Multilicence určena pro běh ve virtuálním prostředí | ANO/NE |
| Licence musí pořízeny v licenčním programu určeném pro státní správu, který umožní  poskytnutí užívacích práv podřízeným organizacím | ANO/NE |
| Licenční model operačního systému umožňujícím běh neomezeného počtu virtuálních strojů | ANO/NE |
| Licence pro 16 procesorových jader | ANO/NE |
| Název a popis dodávaného zboží, odkaz na katalogový list  Doplní dodavatel |  |

### Licence pro virtualizaci

Předmětem plnění je dodávka licencí pro virtualizaci na dodávaný server.

|  |  |
| --- | --- |
| Název | Splněno |
| K dodanému serveru bude dodána i licence serverové virtualizační technologie 100% kompatibilní se stávajícím virtualizačním prostředím úřadu VMWARE 6.5 | ANO/NE |
| 64-bit hypervisor | ANO/NE |
| Licence pro celkem 2 CPU | ANO/NE |
| zajištění vysoké dostupnosti serverů a aplikací, ochrany dat a živé migrace v návaznosti na stávající řešení TC ORP | ANO/NE |
| podpora NAS, NFS, iSCSI a FC protokolů | ANO/NE |
| podpora zapojení do clusteru | ANO/NE |
| Virtuální switching, virtuální síťové karty a teaming síťových karet | ANO/NE |
| podpora VLAN | ANO/NE |
| centrální správa prostřednictvím GUI | ANO/NE |
| nativní podpora Thin Provisioningu | ANO/NE |
| součástí bude podpora na 3 roky s právem na nové verze | ANO/NE |
| Součástí je instalace a konfigurace virtualizace na dodaný HW a začlenění do současné Infrastruktury TC ORP v módu vysoké dostupnosti | ANO/NE |
| Název a popis dodávaného zboží, odkaz na katalogový list  Doplní dodavatel |  |

### Přístupové licence Citrix, CAL licence Windows

Předmětem plnění je rozšíření stávajících licenci Citrix Virtual Apps and Desktops Advanced Edition. Zadavalel si platí pravidelnou roční podporu. Současně je předmětem dodávka licencí síťového prostředí pro dodávaný operační systém pro 150 uživatelů

|  |  |
| --- | --- |
| Název | Splněno |
| Dodávka 20ks licencí Citrix Virtual Apps and Desktops Advanced Edition a Windows terminal server v aktuální verzi | ANO/NE |
| Dodávka 20ks licencí kompatibilních s dodávaným operačním systém v aktuální verzi, licence vázaná na uživatele | ANO/NE |
| Licence musí pořízeny v licenčním programu určeném pro státní správu, který umožní  poskytnutí užívacích práv podřízeným organizacím. | ANO/NE |
| Součástí je instalace licencí, konfigurace a povýšení prostředí Citrix XenDesktop na aktuální verzi | ANO/NE |
| Název a typ dodávaného zboží, odkaz na katalogový list  Doplní dodavatel |  |

### Implementace

Součástí celé dodávky jsou konfigurační práce nezbytné pro zavedení a zprovoznění výšeuvedených systémů. Součástí je i technická dokumentace ke všem dodávaným předmětům plnění. Zároveň bude provedeno školení Administrátorů systému v min. rozsahu 1 den v sídle zadavatele.

|  |  |
| --- | --- |
| Název | Splněno |
| Implementace, technická dokumentace a zaškolení ve výše uvedeném rozsahu | ANO/NE |