Příloha č. 2A zadávací dokumentace

k č. j.: SVS/2018/077258-G

Základní technická specifikace
(veřejná část)

1. Nástroje pro ochranu integrity komunikačních sítí

# FW

Bezpečnostní brána je jednou z klíčových architektonických komponent komplexního řešení. Implementace této komponenty, provozované v režimu vysoké dostupnosti, žadateli umožní:

### Bezpečné a spolehlivé řízení přístupu uživatelů ke službám, provozovaných v jednotlivých segmentech sítě zadavatele

### Provádět základní antivirovou kontrolu datového provozu

### Detekci případných útoků prostřednictvím technologie IPS

### Přistupovat k vnitřním zdrojům zadavatele prostřednictvím technologie VPN

### Ochranu zadavatele před nevyžádanou poštou

# Přepínače

Přepínače budou plošně implementovány na všech 225 koncových pracovišť zadavatele. Celkem se jedná o:

### 32x 1Gbps Ethernet 48 port switch

### 87x 1Gbps Ethernet 24 port switch

### 289x 1Gbps Ethernet 12 port switch

Nedílnou součástí dodávky přepínačů budou SW nástroje, umožňující centrální správu všech aktivních prvků sítě zadavatele a monitoring zadavatelem provozovaných aplikací. V rámci nově pořízených přepínačů bude plošně implementována technologie NAC[[1]](#footnote-1), umožňující řízený přístup[[2]](#footnote-2) uživatelů do komunikační infrastruktury zadavatele.

1. Bezpečnostní software

# Zabezpečení Microsoft Active Directory

Administrace MS AD je v současné době částečně realizována formou externí služby. Nově implementovaný systém přinese možnost účinného a efektivního dohledu nad externími administrátory, kteří tuto službu realizují. Implementace této specializované SW komponenty umožní:

### Zasílání automatizovaných reportů o všech provedených změnách konfigurace MS AD v reálném čase[[3]](#footnote-3) pověřené osobě zadavatele

### Možnost spuštění automatického alertu při nenadálé události

### Kontrolu dlouhodobě nevyužívaných aktivních účtů MS AD

### Kontrolu pravidelných změn hesla u uživatelských účtů, které nejsou řízeny pomocí GPO

### Monitoring případného pokusu o prolomení účtů MS AD pomocí útoku typu „Brute Force“ v reálném čase

# Zabezpečení Microsoft File Systému

Aplikační a uživatelská data Odborného informačního systému jsou umístěna v MS FS a dotčených databázích OIS SVS. Přístupová oprávnění k těmto aktivům jsou přidělována prostřednictvím MS AD. Podobně jako v případě MS AD je i správa OIS SVS částečně realizována formou externí služby. Nově implementovaný systém přinese možnost účinného a efektivního dohledu nad externími administrátory, kteří tuto službu realizují. Implementace této specializované SW komponenty umožní:

### Obousměrnou viditelnost aktuálních přístupových práv[[4]](#footnote-4)

### Systém bude proaktivně navrhovat změny přístupových oprávnění v případě, že je daný uživatel po definovanou dobu nevyužívá

### Systém bude identifikovat přístupová práva, která jsou nastavena přímo na konkrétní uživatele

### Systém bude umožňovat identifikaci práv, odkazujících na již neexistující účet v AD

### Systém bude zobrazovat složky, kde je přerušeno dědění práv z nadřazené složky

### Systém bude na základě analýzy aktivit uživatelů navrhovat vlastníky dotčených dat

### Systém bude sledovat činnost jednotlivých uživatelů a upozorňovat na jejich případné anomální chování

# Identifikace a zabezpečení citlivých dat pomocí klasifikace jejich obsahu

Implementace této specializované SW komponenty přinese možnost klasifikace vybraných citlivých dat OIS SVS dle jejich obsahu. Implementovaný systém bude umožňovat:

### Klasifikaci vybraných citlivých dat na základě souborových metadat[[5]](#footnote-5)

### Klasifikaci vybraných citlivých dat na základě obsahu jednotlivých dokumentů[[6]](#footnote-6)

### Sestavování vlastních klasifikačních pravidel[[7]](#footnote-7), která podporují regulární výrazy

### Sestavování detailních automatizovaných reportů dle zadaných kritérií

### Automatizované reporty musí podporovat možnosti filtrace dle zadaných kritérií[[8]](#footnote-8)

# Ochrana před generickými hrozbami typu „Ransomware“

V posledních několika letech zásadním způsobem narostly případy napadení sdílených úložišť prostřednictvím tak zvaných „Ransomware“, které útočníkovi prostřednictvím napadeného uživatele umožní zašifrovat obsah dat na dotčených datových úložištích. Z tohoto důvodu bude OIS SVS zabezpečen pomocí specializovaného SW řešení, které umožní síťové úložiště OIS SVS efektivně ochránit proti generickým hrozbám, spojeným s plošným znehodnocováním dat. Toto řešení bude zcela automatizované a umožní tak efektivní ochranu v reálném čase.

# Detailní aktivní alertní činnost v reálném čase

Aktivní alerting umožní v reálném čase reagovat na vybrané události, které byly detekovány v rámci činnosti jednotlivých specializovaných SW komponent implementovaného bezpečnostního systému. Implementace tohoto systému umožní:

### Automaticky generovat

### Vytváření vlastních alertních pravidel dle detekovaných událostí[[9]](#footnote-9)

### Rozesílání personalizovaných informací o identifikovaných incidentech[[10]](#footnote-10)

### Spouštění aktivní ochrany systému v případě identifikace bezpečnostního incidentu[[11]](#footnote-11)

# Reportní činnost bezpečnostního SW

Aktivní reporting umožní automatické generování vybraných reportů a jejich distribuci jednotlivým vlastníkům.

# Ochrana koncových bodů

V rámci výkonu činností Státní veterinární správy je používána celá řada koncových zařízení. Jedná se především o stacionární počítače a terminály, přenosné počítače, či mobilní telefony, které v současné době nejsou zabezpečeny proti ztrátě citlivých dat v případě jejich odcizení. Implementovaný systém pro ochranu výše uvedených koncových stanic bude umožňovat:

### Centrální management koncových stanic

### Monitoring uživatelských činností v rámci dotčeného koncového zařízení

### Komplexní šifrování dat koncových zařízení

### Komplexní šifrování dat interní e-mail komunikace

### Kontrolu a správu připojitelných zařízení[[12]](#footnote-12)

### Aplikační kontrolu minimálně na úrovni „Black & White Listing“[[13]](#footnote-13)

### Možnost bezpečného vzdáleného smazání dat na vybraném koncovém zařízení

### Inventarizaci fyzických koncových zařízení

### Snížení provozních nákladů stacionárních koncových zařízení formou úspory elektrické energie[[14]](#footnote-14)

1. Ukládání a zálohování dat OIS

# Ukládání a zálohování dat

Základní parametry nově pořizovaného HW a SW vychází ze současných zkušeností zadavatele, získaných v rámci rutinního provozu a údržby jím provozovaného odborného informačního systému. Jedná se o:

### 1x Diskové pole o minimální celkové hrubé kapacitě 250TB

### 1x Deduplikační zálohovací jednotku o minimální celkové hrubé kapacitě 70TB

### 2x SAN FC 16 MM LCF C 24 port switch

### 1x stojanový rack 42U

### Zálohovací SW

1. Network Access Control. [↑](#footnote-ref-1)
2. Prostřednictvím protokolu 802.1x. [↑](#footnote-ref-2)
3. Například přidání či odebrání libovolného uživatele či administrátora z/do libovolné skupiny, změny GPO, založení nových uživatelských účtů, … [↑](#footnote-ref-3)
4. Administrátor systému tak bude například schopen identifikovat jednotlivé kategorie přístupových práv napříč všemi dotčenými úložišti, a to jak ze strany uživatele či skupiny, tak ze strany jednotlivých souborů či souborových složek. [↑](#footnote-ref-4)
5. Například dle typu dokumentu. [↑](#footnote-ref-5)
6. Například rodná čísla, data narození, … [↑](#footnote-ref-6)
7. Například vyhledání souborů větších než definovaný objem a zároveň nepoužívaných déle jak definovaný čas. [↑](#footnote-ref-7)
8. Například filtr dle role vlastníka souboru v MS AD. [↑](#footnote-ref-8)
9. Události budou detekovány na základě výstupů implementovaných specializovaných SW komponent (MS AD, MS FS, Klasifikace obsahu dat, Ochrana přad generickými hrozbami typu „Ransomware“). [↑](#footnote-ref-9)
10. Minimálně ve formátu CSV, PDF a XML formou plně automatizované řízené distribuce prostřednictvím personalizované přílohy elektronické pošty, či uložení na vybrané místo sdíleného datového úložiště. [↑](#footnote-ref-10)
11. Například požadavek na automatické zneaktivnění daného účtu v AD, odpojení portu dotčeného zařízení na přepínači, či vypnutí napadeného zařízení. Tento požadavek taktéž determinuje budoucí výběr použitých HW komponent (FW, Přepínače), které je třeba s funkčními a nefunkčními požadavky na bezpečnostní SW plně integrovat. [↑](#footnote-ref-11)
12. Například USB, FireWire, WLAN, Bluetooth, CD, DVD, … [↑](#footnote-ref-12)
13. Seznam explicitně povolených, či zakázaných aplikací. [↑](#footnote-ref-13)
14. Například formou automatického vypínání stacionárních zařízení v mimopracovní době. [↑](#footnote-ref-14)