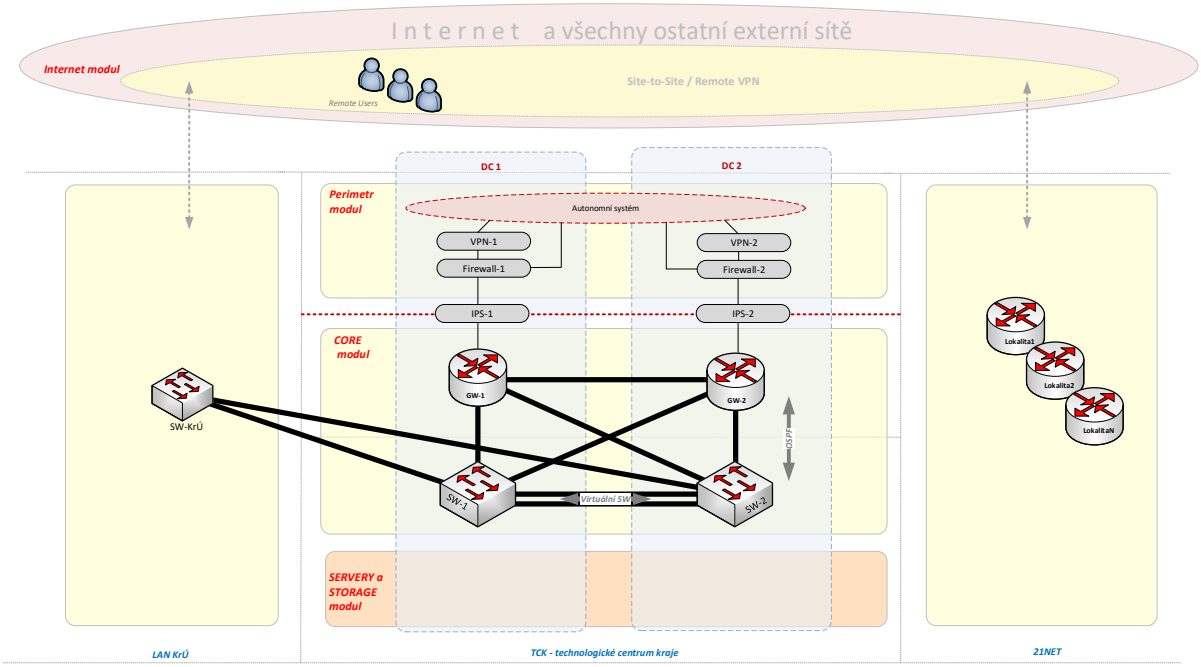
Příloha č. 1: Podrobné vymezení díla

Dodávka a implementace řešení pro zaznamenávání činnosti VIP účtů a zajištění následné podpory

Obsah

Popis současného prostředí

Základní schema aktuálního stavu



Poskytnutá virtualizační platforma

Pokud je u jednotlivých bodů nabízena možnost řešení v podobě virtualizované appliance (VApp) nebo virtual machine (VM), je možné v rámci technologického centra Objednatele (TC KÚZK, TCK) nabídnout prostředí VMWare VSphere 6.0 a OS MS Windows Server 2012/2016 DataCenter Edition. Pro chod řešení může být také poskytnuta databáze / instance na stávajícím MS SQL 2014/2016 řešení TC KÚZK.

Podrobné kapacitní možnosti pro VApp/VM a SQL (počet vCPU, velikost operační paměti, úložiště…) jsou specifikovány níže.

1. Zavedení zaznamenávání činností VIP účtů administrátorů a uživatelů třetích stran

Předmětem tohoto řešení je pořízení a zavedení nového komplexního systému pro monitoring činnosti privilegovaných uživatelů (vyjmenovaní uživatelé, administrátoři, dodavatelé, externisté a kdokoliv, kdo má přístup do systému). Zároveň také zajistí konkrétní záznam činnosti definovaného účtu včetně screenshotů prováděných činností a vytvoří případně i data a záznamy o činnosti konkrétního definovaného účtu, které mohou být použity ve formě videosekvence pro dokazování porušení pravidel práce s daty a podobně.

Systém identifikuje všechny nové relace na serveru a přiřadí je k specifickému uživateli. Během relace jsou veškeré aktivity nahrávány přesně tak, jak je uživatel vidí na své obrazovce. Kromě videozáznamu jsou převáděny do podoby textových logů pro snadné budoucí vyhledávání logů i z aplikací, které žádné interní logy nemají. To výrazně usnadňuje vyhledávání požadovaných událostí. Přehledné reporty následně chronologicky zobrazují seznam provedených akcí včetně odkazů pro přehrání příslušného videa. Aktivity lze monitorovat na širokém spektru protokolů a prostředí. Systém umožňuje nastavení pravidel pro pořizování záznamů podle aplikací, uživatele, serveru, URL, různých skupin.

Vygenerované přehledné reporty chronologicky zobrazují seznam provedených akcí včetně odkazů pro přehrání příslušného videa.

Minimální požadované funkce a vlastnosti řešení

- celé řešení bude podporovat provoz ve virtualizovaném prostředí KÚZK
- záznam všech aktivit spojených s použitím privilegovaného účtu na monitorovaných systémech (servery a koncové stanice)
    - možnost záznamu grafickou formou (zejména screenshot, videozáznam)
    - v rámci nahrávky jsou zaznamenávány uživatelské vstupy (key-logging) a výstupy na obrazovku
    - přiřazení nových relací patřičným uživatelům
- získávání detailních metadat během nahrávané uživatelské relace (stisknuté klávesy, názvy aktivních oken, textové řetězce z oblastí, kde proběhla aktivita (např. klik myší na definované tlačítko/záložku/…)
- v metadatech musí být možné vyhledávat dle textových řetězců
- ukládání nahraných uživatelských relací na definované úložiště Objednatele v šifrované podobě
- přehlednou správu politik pro monitoring nejen privilegovaných účtů
- počet monitorovaných systémů:
    - 1x Terminal server (Windows Server 2012 R2 a vyšší) – Jump Server GW
    - 5x Published App Agent – určeno pro monitoring publikovaných aplikací, licence pro každý terminálový server
    - 10x Windows Server (Windows Server 2012 R2 a vyšší)
    - 5x Windows Desktop (Windows 7 Enterprise a Windows 10 Enterprise)
- aplikace musí umožnit správu rolí (auditor, správce apod.)
- uživatelé mohou být dle nastavení Objednatele upozorněni na skutečnost, že jejich aktivita je nahrávána
- auditování, monitoring a nahrávání aktivit administrátorů na serverech při vzdáleném i lokálním přihlášení
- auditování, monitoring a nahrávání aktivit externích uživatelů vykonávající vzdálenou správu v LAN Objednatele pomocí předřazené virtuální administrační stanice nebo terminálového serveru
- auditování, monitoring a nahrávání aktivit vybraných interních zaměstnanců využívajících virtuální desktopy, počítače nebo notebooky
- schopnost zpětně přehrávat uživatelské relace ve formě videosekvence
- schopnost exportu nahraných uživatelských relací (formou printscreenů obrazovek a to včetně metadat) pro tvorbu dokumentace, nebo prokazování incidentů
- každá událost v logu, má vazbu pomocí URL adresy na konkrétní místo videosekvence, kde k této události došlo
- integrována funkce šifrování nahraných uživatelských relací, před jejich uložením
- integrována funkce integrity nahraných uživatelských relací, pokud je integrita porušena, jsou tyto relaci v přehledu označeny
- politikou je možné definovat uživatele, kteří budou, nebo naopak nebudou nahrávání

- politikou je možné definovat aplikace (aplikace, nebo URL adresa v případě webových aplikací), které budou, nebo naopak nebudou nahrávány
- integrovaný reporting, s možností tvorby vlastních reportů o aktivitách uživatelů, vč. exportu do CSV nebo XLS nebo XML nebo HTML pro následné analýzy

Požadované integrace:

- do MS AD KÚZK
- do provozovaného SIEM KÚZK

Poskytnutá virtualizační platforma a její kapacitní možnosti

Pro chod VApp/VM v prostředí TCK KÚZK bude možnost vyhrazení HW prostředků s následující charakteristikou:

Technická specifikace poskytnutého prostředí – maximální hodnoty	
počet podporovaných vCPU	8
počet virtuálních NIC	2
velikost úložiště virtuálního stroje / při integraci na SIEM	80 GB / 500 GB
velikost operační paměti virtuálního stroje	16 GB
velikost databáze / instance na sdíleném MS SQL 2014/2016 řešení KÚZK	10 GB

2. Požadované služby

2.1 Služby v rámci dodávky

V rámci dodávky budou požadovány následující služby:

- Projektové řízení dodávky řešení.
- Zpracování návrhu řešení implementace jednotlivých částí – Prováděcí projekt včetně návrhu řešení specifikovaný v Příloze č. 3 Povinná struktura Prováděcího projektu včetně návrhu řešení.
- Dodávka, implementace, instalace, zapojení a konfigurace všech částí dle Prováděcího projektu včetně návrhu řešení.
- Vytvoření a předání Objednateli zálohy konfigurace.
- Ověření funkčnosti dodaného řešení a jeho částí.
- Dodávka dokumentace dodaného vybavení a jeho částí.
- Kvalifikované seznámení administrátorů – seznámení s funkcionalitami, obsluhou dodávaného řešení a jeho budoucím provozem v rozsahu minimálně 1MD.
- Implementace metodik a pracovních postupů.
- Provedení zkušebního provozu.
- Podpora provozu dle Přílohy č. 4: Podmínky zajištění podpory provozu díla

2.2 Dokumentace

V rámci plnění bude dodána zhotovitelem kompletní dokumentace řešení (dokumentace může být jedním dokumentem, nicméně musí obsahovat všechny relevantní informace) obsahující minimálně:

- Podrobná systémová a bezpečnostní dokumentace (administrátorská dokumentace) v českém jazyce:
    - popis skutečného provedení řešení min. ve struktuře dle Prováděcího projektu včetně návrhu řešení;
    - princip aktualizace;
    - seznam licencí.
- Kompletní provozní dokumentace ke všem částem v českém nebo anglickém jazyce.

3. Seznam zkratek a pojmů

Zkratka	Význam, výklad
AD	Active Directory – autentikační a adresářový systém pro platformu Windows
CPU	Central Processing Unit – procesor počítače
CSV	Comma Separated Value – formát dat (souboru)
GB	Giga Byte - jednotka množství dat v informatice
HTML	Hypertext Markup Language – jazyk pro tvorbu webových stránek
KÚZK	Krajský úřad Zlínského kraje
LAN	Local Area Network – lokální počítačová síť
MD	Man Day – čas odpovídající práci jedné osoby po dobu jednoho pracovního dne
MS	Microsoft
NIC	Network Interface Controller – síťová karta
SIEM	Security Information and Event Management
SQL	Structured Query Language – jazyk pro práci s databázemi
TC	Technologické centrum
TCK	Technologické centrum kraje
VApp	virtualizovaná appliance
vCPU	virtual Central Processing Unit – virtuální procesor počítače
VIP	Very Important Person
VM	Virtual Machine
XLS	Excel Binary File Format – původní formát aplikace Microsoft Excel

XML	eXtensible Markup Language - obecný značkovací jazyk