**Príloha č. 15**

Zvýšenie úrovne informačnej a kybernetickej bezpečnosti ÚJD SR

Časť č. 1 predmetu zákazky: Zvýšenie úrovne informačnej a kybernetickej bezpečnosti ÚJD SR – časť 1

Technické parametre riešenia

## Pokyny pre vyplnenie „Tabuľky pre hodnotenie technických parametrov riešenia“

Pokyny pre vyplnenie „Tabuľky pre hodnotenie technických parametrov riešenia“:

1. Záujemca vyplní „Údaje o dodávanom zariadení/systéme“ (v prípade viacerých rôznych zariadení/systémov vyplní údaje o všetkých typoch), t. j.:

* Výrobca
* Model
* Konfigurácia
* Odkaz na produktovú dokumentáciu na stránkach výrobcu (link), z ktorej je možné overiť parametre ponúkaných produktov

1. Záujemca vyplní stĺpec „Splnenie požiadaviek“, pričom splnenie pre každý hodnotený parameter vyhodnotí a uvedie „áno“ v prípade splnenia alebo „nie“ v prípade nesplnenia daného parametra.
2. V stĺpci „Hodnota parametra“ Záujemca uvedenie konkrétnu hodnotu daného parametra pre ním ponúkaný produkt.

Záujemca môže zapisovať iba do polí tabuľky, ktoré nie sú vyfarbené šedou farbou.

# Podrobná špecifikácia predmetu zákazky

Všetky parametre (pokiaľ nie je explicitne stanovené inak) sú uvedené ako minimálne požiadavky.

V prípade, že je uvedená akákoľvek odvolávka na konkrétny produkt, je možné ponúknuť aj jeho ekvivalent.

## Centrálny manažment PC

Aktuálne je nasadený iba manažment distribúcie aplikácií. Je obmedzený na určité operačné systémy, je limitovaný funkciami a miera automatizácie činností je malá. Požadovaný manažment pracovných staníc bude s vysokou mierou automatizácie, umožní jednotnú správu verzií operačných systémov a ich súčastí, aplikácií a ich verzií. Ďalej umožní riadenie aktualizácií.

### Softvér pre centrálny manažment PC

Údaje o ponúkanom zariadení/systéme:

Výrobca: <doplniť>

Model: <doplniť>

Konfigurácia: <doplniť detailnú konfiguráciu ponúkaného zariadenia/systému>

Odkaz na produktovú dokumentáciu na stránkach výrobcu (link): <doplniť link, kde je možné overiť parametre ponúkaných produktov>

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Manažované OS | Microsoft Windows rôzne verzie |  |  |
| Počet klientov (manažovaných PC) | 200 |  |  |
| Klienti | Import klientov  Vyhľadávanie klientov  Vytváranie skupín klientov  Monitorovanie aktivity klientov  Reporty  Vytváranie vlastných prehľadov |  |  |
| Hardvérová inventarizácia | Konfigurácia parametrov pre hardvérovú inventarizáciu  Plánovanie vykonania v rôznych časových intervaloch  Zaslanie výsledkov z klienta po obnovení dostupnosti servera  Ad-hoc inventarizácia vyvolaná z konzoly správcu  História inventarizácie uchovávaná min. 90 dní  Výsledky poslednej inventarizácie uchovávané neobmedzený čas  Reporty  Vytváranie vlastných prehľadov |  |  |
| Softvérová inventarizácia | Konfigurácia parametrov pre softvérovú inventarizáciu (typy súborov, priečinky)  Plánovanie vykonania v rôznych časových intervaloch  Zaslanie výsledkov po obnovení dostupnosti servera  Ad-hoc inventarizácia vyvolaná z konzoly správcu  Výsledky poslednej inventarizácie uchovávané neobmedzený čas  Reporty  Vytváranie vlastných prehľadov |  |  |
| Operačné systémy | Automatická inštalácia operačných systémov a inštalácia na vyžiadanie  Automatická reinštalácia operačných systémov a reinštalácia na vyžiadanie so zachovaním dát a nastavení  Automatický upgrade a upgrade na vyžiadanie operačných systémov so zachovaním dát a nastavení  Inštalácia ovládačov  Vyhodnocovanie úspešnosti inštalácie, reinštalácie a upgrade  Reporty  Vytváranie vlastných prehľadov. |  |  |
| Aktualizácie operačných systémov | Automatická inštalácia aktualizácií operačných systémov (patchov) pre rôzne skupiny počítačov  Inštalácia aktualizácií na vyžiadanie  Fázová inštalácia aktualizácií  Offline aktualizácia obrazov alebo balíčkov operačných systémov  Vyhodnocovanie úspešnosti inštalácie  Reporty  Vytváranie vlastných prehľadov |  |  |
| Aplikácie | Automatická inštalácia aplikácií pre rôzne skupiny počítačov alebo používateľov  Inštalácia aplikácií na vyžiadanie pre rôzne skupiny počítačov alebo používateľov  Automatický upgrade aplikácií pre rôzne skupiny počítačov alebo používateľov  Automatická odinštalácia aplikácií pre rôzne skupiny počítačov alebo používateľov  Možnosti inštalácie štandardných aj moderných aplikácií z Microsoft Store  Vyhodnocovanie úspešnosti inštalácie, upgrade a odinštalácie aplikácií  Reporty  Vytváranie vlastných prehľadov |  |  |
| Monitorovanie používania softvéru | Výber programov, ktorých používanie sa má monitorovať  Monitorovanie používania  Vyhodnocovanie používania  Reporty  Vytváranie vlastných prehľadov |  |  |
| Zhoda s požiadavkami | Definovanie požiadaviek na PC  Vyhodnocovanie požiadaviek  Automatické riešenie nezhôd  Monitorovanie  Reporty |  |  |
| Skripty PowerShell | Vytváranie a import skriptov PowerShell  Spúšťanie skriptov na skupinu počítačov alebo jednotlivé počítače  Monitorovanie spúšťania skriptov |  |  |
| Monitorovanie | Monitorovanie systému a jeho jednotlivých komponentov  Konfigurácia alertov pre kritické udalosti  Zasielanie e-mailových notifikácií. |  |  |
| Zabezpečenie | Prístup na základe rolí a skupín objektov  Vytváranie vlastných rolí s definovanými oprávneniami |  |  |
| Zálohovanie a obnova | Zálohovanie systému, konfigurácie a dát pre prípad požiadavky na obnovu |  |  |

### Vypracovanie návrhu riešenia centrálneho manažmentu PC

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Vypracovanie návrhu riešenia | **Dokument s obsahom:**  Popis funkcionality, ktorá sa bude používať  Používané služby a komponenty  Návrh architektúry riešenia  Návrh topológie riešenia  Požiadavky na licencie  Hardvérové požiadavky  Softvérové požiadavky  Požiadavky na komunikáciu  Požiadavky na infraštruktúrne služby (Active Directory, group policy a ďalšie)  Požiadavky na aktualizáciu Active Directory a úpravu príslušných GPO  Popis konfigurácie jednotlivých funkcií, služieb a komponentov  Zálohovanie a obnova systému, konfigurácie a dát |  |  |

### Konfigurácia centrálneho manažmentu PC

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Konfigurácia | **Konfigurácia nasledovných častí:**  Služby a komponenty pre všetku používanú funkcionalitu  Plánovanie vyhľadávania klientov  Konfigurácia parametrov pre hardvérovú a softvérovú inventarizáciu, ich plánovanie  Konfigurácia inštalácie aktuálnej a predchádzajúcej verzie operačného systému Windows 10 alebo jeho nasledovníka  Konfigurácia reinštalácie na túto verziu a upgrade na túto verziu so zachovaním dát a nastavení  Konfigurácia systému pre inštaláciu aktualizácií operačných systémov, konfigurácia fázovej inštalácie  Konfigurácia systému pre inštaláciu aplikácií, príprava inštalácie min. 3 štandardných aplikácií, 1 upgrade aplikácie a 1 aplikácie z Microsoft Store  Konfigurácia monitorovania používania min. 3 aplikácií  Konfigurácia alertov pre kritické udalosti a e-mailových notifikácií  Konfigurácia rolí pre prístup, minimálne globálny správca a oprávnenia na prezeranie  Konfigurácia zálohovania  Aktualizácia Active Directory a úprava príslušných GPO |  |  |

### Overovanie a ladenie centrálneho manažmentu PC

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Overovanie a ladenie | Vyhľadávanie klientov  Výsledky hardvérovej inventarizácie  Výsledky softvérovej inventarizácie  Inštalácia operačného systému, reinštalácia a upgrade operačného systému, ich monitorovanie a vyhodnotenie  Mesačná inštalácia aktualizácií operačných systémov, ich monitorovanie a vyhodnotenie  Offline aktualizácia obrazu alebo balíčka operačného systému  Inštalácia pripravených aplikácií min. na 3 počítače, monitorovanie a vyhodnotenie inštalácie  Výsledky monitorovania používania aplikácií  Vyhodnotenie alertov a e-mailových notifikácií  Monitorovanie zálohovania.  Obnova systému v oddelenom prostredí |  |  |

### Vypracovanie dokumentácie riešenia centrálneho manažmentu PC

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Vypracovanie dokumentácie riešenia | Popis funkcionality, ktorá sa používa  Používané služby a komponenty  Popis architektúry riešenia a obrazová schéma  Popis topológie riešenia a obrazová schéma  Používané licencie  Popis hardvérovej konfigurácie  Zoznam nainštalovaného softvéru  Popis komunikácie  Popis používaných infraštruktúrnych služieb (Active Directory, group policy a ďalšie)  Popis konfigurácie jednotlivých funkcií, služieb a komponentov  Popis zálohovania a obnovy systému, konfigurácie a dát  Vypracovanie používateľskej príručky |  |  |

### Zaškolenie administrátorov centrálneho manažmentu PC

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Zaškolenie administrátorov | Konfigurácia systému a komponentov  Monitorovanie systému a komponentov  Plánovanie vyhľadávania klientov  Konfigurácia parametrov pre hardvérovú a softvérovú inventarizáciu, ich plánovanie a výsledky  Konfigurácia inštalácie, reinštalácie a upgrade operačného systému, priradenie skupine, spustenie, monitorovanie a vyhodnotenie  Konfigurácia systému pre inštaláciu aktualizácií operačných systémov, priradenie skupine, spustenie, monitorovanie a vyhodnotenie  Konfigurácia systému pre inštaláciu aplikácií, príprava inštalácie aplikácií, priradenie skupine, spustenie, monitorovanie a vyhodnotenie  Konfigurácia monitorovania používania aplikácií, vyhodnotenie  Konfigurácia alertov pre kritické udalosti a e-mailových notifikácií  Konfigurácia rolí pre prístup  Reporty  Vytváranie vlastných prehľadov  Konfigurácia zálohovania  Postup pre obnovu systému |  |  |

## Centrálny systém zálohovania dát

Zálohovanie je aktuálne riešené pre centrálne systémy iba zálohovaním na disky. Implementáciou budúceho centrálne riadeného zálohovania budú ochránené dáta, zálohovanie bude bez zásahu používateľov a bude pravidelné. Ochrana pred zlyhaním hardvéru bude vysoká, nakoľko budú dáta ukladané na 2 úložiská v rôznych lokalitách a budú zálohované aj na pásky s možnosťou ukladania v inej lokalite.

Požadovaná architektúra zálohovacieho systému obsahuje zálohovací server s vlastným diskovým úložiskom v každej lokalite a páskovú knižnicu na ukladanie kópií dát v primárnej lokalite. Dáta uložené na diskové úložisko musia byť pravidelne replikované do druhej lokality za účelom zníženia rizika straty dát pri výpadku diskového poľa, prípadne poškodenia dát. Zároveň musí byť umožnená obnova dát zo záložnej lokality pri výpadku zálohovacieho servera v primárnej lokalite.

### Zálohovací softvér pre zálohovanie virtuálnych serverov

Požadujeme dodávku licencií pre **50 virtuálnych serverov**, ktoré budú súčasťou Virtualizačnej platformy pre prevádzku bezpečnostných systémov.

Údaje o ponúkanom zariadení/systéme:

Výrobca: <doplniť>

Model: <doplniť>

Konfigurácia: <doplniť detailnú konfiguráciu ponúkaného zariadenia/systému>

Odkaz na produktovú dokumentáciu na stránkach výrobcu (link): <doplniť link, kde je možné overiť parametre ponúkaných produktov>

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Spôsob zálohovania | Zálohovanie virtuálnych serverov prostredníctvom integrácie s virtualizačnou vrstvou bez nutnosti inštalácie zálohovacieho agenta na každý virtuálny server  Možnosť zálohovania ľubovoľného virtuálneho servera pomocou agenta |  |  |
| Požadované funkcie | Kompresia zálohovaných dát  Deduplikácia zálohovaných dát  Možnosť centrálneho riadenia zálohovacích politík  Možnosť zaradenia jednotlivých zálohovaných serverov do skupín s rovnakou politikou zálohovania  Možnosť ukladania dát na páskové zariadenia  Možnosť replikácie záloh do inej vzdialenej lokality  Centrálna konzola s možnosťou monitorovania systému a reportovania |  |  |
| Licencovanie | Licencovanie na zálohovanie **minimálne 50 virtuálnych serverov** a akéhokoľvek objemu zálohovaných dát |  |  |
| Záručné podmienky | SW podpora na celkové obdobie 3 rokov s právom na aktualizácie verzií a opravu chýb |  |  |

### Zálohovací softvér pre zálohovanie samostatných serverov a pracovných staníc používateľov

Predmetom dodávky je zálohovací softvér pre **8 samostatných serverov** (nevirtualizované), ktoré budú zálohované na centrálny zálohovací systém.

Údaje o ponúkanom zariadení/systéme:

Výrobca: <doplniť>

Model: <doplniť>

Konfigurácia: <doplniť detailnú konfiguráciu ponúkaného zariadenia/systému>

Odkaz na produktovú dokumentáciu na stránkach výrobcu (link): <doplniť link, kde je možné overiť parametre ponúkaných produktov>

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Podpora operačných systémov | Microsoft Windows Server 2016 a vyššie  Linux (Red Hat, CentOS, Fedora, Ubuntu, Debian, SUSE, ClearOS) |  |  |
| Podpora aplikácií | Microsoft SQL server  Microsoft Active Directory  Oracle DB |  |  |
| Ďalšie vlastnosti | Riadenie centrálnym komponentom zálohovacieho systému  Licencovanie nezávislé na množstve zálohovaných dát  Deduplikácia a kompresia zálohovaných dát  Možnosť obnovy na nový server (Bare metal recovery)  Možnosť obnovy na iný server podobnej konfigurácie  Možnosť obnovy na virtuálny server |  |  |
| Záručné podmienky | SW podpora na celkové obdobie 3 rokov s právom na aktualizácie verzií a opravu chýb |  |  |

V rámci predmetu dodávky je požadované zálohovanie pracovných staníc v počte 200 ks, ktoré bude vykonávané na centrálny zálohovací systém a pre ukladanie dát z týchto pracovných staníc platia rovnaké požiadavky (deduplikácia, kompresia, replikácia na druhú lokalitu) ako pre dáta z fyzických a virtuálnych serverov.

Údaje o ponúkanom zariadení/systéme:

Výrobca: <doplniť>

Model: <doplniť>

Konfigurácia: <doplniť detailnú konfiguráciu ponúkaného zariadenia/systému>

Odkaz na produktovú dokumentáciu na stránkach výrobcu (link): <doplniť link, kde je možné overiť parametre ponúkaných produktov>

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Podpora operačných systémov | Microsoft Windows 10 a vyšší  Linux (Red Hat, CentOS, Fedora, Ubuntu, Debian, SUSE, ClearOS)  Mac OS 10.15 a vyššie |  |  |
| Počet zálohovaných pracovných staníc | 200 |  |  |
| Ďalšie vlastnosti | Riadenie centrálnym komponentom zálohovacieho systému  Licencovanie nezávislé na množstve zálohovaných dát  Deduplikácia a kompresia zálohovaných dát  Možnosť obnovy na nový počítač (Bare metal recovery)  Možnosť obnovy na inú pracovnú stanicu podobnej konfigurácie |  |  |
| Záručné podmienky | SW podpora na celkové obdobie 3 rokov s právom na aktualizácie verzií a opravu chýb |  |  |

### Pásková knižnica a zálohovacie médiá

Údaje o ponúkanom zariadení/systéme:

Výrobca: <doplniť>

Model: <doplniť>

Konfigurácia: <doplniť detailnú konfiguráciu ponúkaného zariadenia/systému>

Odkaz na produktovú dokumentáciu na stránkach výrobcu (link): <doplniť link, kde je možné overiť parametre ponúkaných produktov>

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Prevedenie | Modulárne zariadenie s veľkosťou max. 3U montovateľné do štandardnej dátovej skrine (pre minimálnu konfiguráciu) |  |  |
| Páskové mechaniky | Minimálne 2x LTO Ultrium 8 alebo novšie |  |  |
| Počet slotov | Minimálne 40 slotov pre páskové médiá LTO |  |  |
| Pripojenie | Minimálne 16Gbit/s Fibre channel pre každú mechaniku  Ethernet RJ-45 pre vzdialenú správu |  |  |
| Ďalšie vlastnosti | Možnosť rozšírenia pomocou expanzných modulov  Automatická voľba cesty k robotickej mechanike (auto controll path)  Redundancia dátového pripojenia (data path failover) |  |  |
| Záručné podmienky | 3 roky s pokrytím 24x7 a garantovanou dobou opravy nasledujúci pracovný deň |  |  |
| Príslušenstvo | 40 ks médií LTO Ultrium 8 alebo novšie  2 ks čistiacich médií |  |  |

### Diskové pole pre ukladanie záloh

Diskové pole bude slúžiť ako diskové úložisko pre zálohovací server, na ktoré budú ukladané samotné zálohy pre zabezpečenie čo najrýchlejšej obnovy. Toto úložisko musí byť plne podporované navrhovaným zálohovacím systémom. Riešenie bude obsahovať diskové pole na ukladanie záloh na každej lokalite (celkovo 2 ks identických úložísk).

Údaje o ponúkanom zariadení/systéme:

Výrobca: <doplniť>

Model: <doplniť>

Konfigurácia: <doplniť detailnú konfiguráciu ponúkaného zariadenia/systému>

Odkaz na produktovú dokumentáciu na stránkach výrobcu (link): <doplniť link, kde je možné overiť parametre ponúkaných produktov>

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Kapacita | Minimálna využiteľná kapacita 70 TB s využitím distribuovaného RAID6 |  |  |
| Použité disky | Požadujeme disky 7200 RPM NearLine SAS |  |  |
| Prevedenie | Plne redundantné diskové pole o celkovej veľkosti max. 2U montovateľné do štandardnej dátovej skrine |  |  |
| Redundancia | Všetky kľúčové komponenty sú redundantné |  |  |
| Rozšíriteľnosť | Systém umožňuje ďalšie rozširovanie fyzickej kapacity minimálne na 5-násobok dodávaného počtu diskov |  |  |
| Podpora RAID | Podpora pre hybridné módy RAID (10, 50, 60) alebo distribuované DRAID 5, 6, pričom „hot spare“ priestor je distribuovaný cez všetky diskové moduly v RAID skupine (nie dedikovaný globálny hot spare disk)  Umožňuje online rozšírenie RAID skupiny pridaním len jedného disku (bez prerušenia chodu aplikácií) |  |  |
| Údržba za chodu | Online upgrade mikrokódov kontrolérov, flash/SSD modulov a rotačných diskov a online výmena kľúčových komponentov diskového poľa |  |  |
| Replikácia | Umožňuje dátovú replikáciu pre požadovanú kapacitu v synchrónnom a asynchrónnom móde medzi dvoma až troma lokalitami s časovo neobmedzeným licenčným pokrytím na požadovanú kapacitu |  |  |
| Host konektivita | Požadujeme pripojenie pomocou Fibre Channel, minimálne 16 Gbit/s  Podpora pre 16Gb/s FC, 10GbE iSCSI, SAS, 25Gb/s iSER iSCSI |  |  |
| Vyrovnávacia pamäť | Vyrovnávacia systémová pamäť cache minimálne 64 GB (nie flash cache) |  |  |
| Rozšírené funkcie | Umožňuje virtualizáciu internej diskovej kapacity a thin provisioning s časovo neobmedzeným licenčným pokrytím na požadovanú kapacitu  Umožňuje automatický load balancing LUN –ov v rámci single tierového storage poolu (optimalizácia rozloženia záťaže)  Umožňuje vytváranie lokálnych kópii dát (snapshot-ov a klonov) s časovo neobmedzeným licenčným pokrytím na požadovanú kapacitu |  |  |
| Správa diskového poľa | Podpora SNMP, e-mail notifikácia a podpora call-home  Diskové pole musí obsahovať GUI prostredníctvom HTTPS, CLI prostredníctvom SSHv2 a všetky potrebné multipath ovládače pre požadované podporované OS  Podporuje RESTfull Api a CSI  Navrhované diskové pole musí umožňovať pripojenie ku cloudovej službe výrobcu diskového poľa a musí umožňovať monitoring výkonu, kapacity a proaktívny health monitoring navrhovaného diskového poľa. Uvedená cloudová služba musí podporovať automatizáciu procesu servisnej podpory s cieľom dosiahnutia rýchlejšieho riešenia HW a SW problémov (ako napr. automatická kolekcia logov, filtrovanie udalostí, vytváranie a manažment servisných ticketov) |  |  |
| Záručné podmienky | SW a HW podpora na obdobie 3 rokov s pokrytím 24x7 a garantovanou dobou odstránenia poruchy nasledujúceho pracovného dňa |  |  |

### Inštalácia a konfigurácia zálohovacieho systému a replikácie zálohovaných údajov do druhej lokality

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Detailný návrh riešenia centrálneho zálohovacieho systému | Analýza požiadaviek  Návrh architektúry a konfigurácie zálohovacieho systému  Návrh zálohovacích politík  Návrh postupov pre zálohovanie a obnovu jednotlivých typov dát  Návrh spôsobu replikácie dát medzi lokalitami a zabezpečenia kópií na páskovú knižnicu  Návrh testovacích scenárov pre vykonanie testov zálohovania a obnovy  Návrh postupov pre inštaláciu a konfiguráciu agentov pre samostatné servery a pracovné stanice  Návrh pracovných postupov pre údržbu systému |  |  |
| Inštalácia a konfigurácia komponentov zálohovacieho systému | Inštalácia zálohovacieho systému (server) na oboch lokalitách  Konfigurácia systému  Pripojenie a konfigurácia úložísk dát  Konfigurácia používateľov a prístupových práv |  |  |
| Inštalácia a konfigurácia agentov pre samostatné servery a pracovné stanice | Inštalácia agentov  Konfigurácia pripojenia na zálohovací server  Test konektivity |  |  |
| Konfigurácia zálohovacích politík | Konfigurácia zálohovacích politík (retenčné doby a počty ukladaných záloh)  Konfigurácia plánovaných úloh (zálohovania) pre jednotlivé typy dát |  |  |
| Konfigurácia replikácie dát medzi lokalitami | Konfigurácia replikácie  Test výkonnosti replikácie |  |  |
| Test zálohovacieho systému | Skúšobné vykonanie zálohy jednotlivých typov dát  Skúšobné vykonanie obnovy zazálohovaných dát |  |  |
| Vypracovanie prevádzkovej dokumentácie | Dokumentácia musí obsahovať konfiguráciu systému a prevádzkové postupy pre administrátorov |  |  |
| Zaškolenie obsluhy | Zaškolenie v dĺžke trvania 1 deň pre ľubovoľný počet administrátorov v priestoroch Objednávateľa |  |  |

**Centrálny systém zálohovania dát (Zálohovacie servery)**

Zálohovacie servery budú slúžiť pre prevádzku zálohovacieho systému. Požadujeme po jednom zálohovacom serveri pre každú lokalitu.

### Operačný systém zálohovacieho servera

Údaje o ponúkanom zariadení/systéme:

Výrobca: <doplniť>

Model: <doplniť>

Konfigurácia: <doplniť detailnú konfiguráciu ponúkaného zariadenia/systému>

Odkaz na produktovú dokumentáciu na stránkach výrobcu (link): <doplniť link, kde je možné overiť parametre ponúkaných produktov>

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Operačný systém | Microsoft Windows 2019 Standard s pokrytím pre všetky jadrá osadených CPU |  |  |

### Zálohovací server

Údaje o ponúkanom zariadení/systéme:

Výrobca: <doplniť>

Model: <doplniť>

Konfigurácia: <doplniť detailnú konfiguráciu ponúkaného zariadenia/systému>

Odkaz na produktovú dokumentáciu na stránkach výrobcu (link): <doplniť link, kde je možné overiť parametre ponúkaných produktov>

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Prevedenie | Optimalizovaný pre umiestnenie do 19" dátového rozvádzača (racku), výška max. 1U  Uchytenie servera v racku na výsuvných koľajniciach |  |  |
| Požiadavky na procesor(y) | Osadený minimálne jeden procesor s parametrami: min. 16 jadier.  Server musí byť preukázateľne schopný dosiahnuť výsledok v teste SPECrate®2017\_int\_base aspoň 160 bodov.Údaj o výkone musí byť preukázateľný pre konkrétny ponúkaný server na verejne dostupnej stránke https://www.spec.org |  |  |
| Systémová pamäť | Server disponuje min. 16 využiteľnými pamäťovými slotmi, pamäť celkovo rozšíriteľná do min. 2TB  Osadená kapacita: min. 128GB DDR4 3200MHz Registered DIMM, s funkciou detekcie a opravy multibitových chýb, zrkadlenia pamätí, on-line spare pamäte |  |  |
| Subsystém pevných diskov | Server musí podporovať budúce rozšírenie interných pozícií pre 2,5" disky typu hot-swap do počtu min. 12 ks bez potreby pripojenia externej diskovej police.  Osadené 2x min. 480GB SATA SSD typu m.2 priamo na matičnej doske, nakonfigurované v RAID 1.  Min. prepisová kapacita 1324TB alebo min 1,5 DWPD. Minimálne výkonnostné parametre disku: 85tis IOPS pri čítaní (4kB bloky) a 36tis pri zápise (4kB bloky). |  |  |
| NVMe | Podpora NVMe diskov |  |  |
| Sieťové adaptéry | Min. 1x 2-portový 10/25Gbps ethernet adaptér pre pripojenie k externému prostrediu s rozhraním SFP+, adaptér typu onboard alebo ako PCIe rozširujúca karta  Min. 1x 2-portový 1Gbps ethernet adaptér pre pripojenie k externému prostrediu metalickým rozhraním typu RJ45  Dedikovaný port pre manažment servera |  |  |
| FibreChannel adaptér | Min. 1x dual port 16Gbps Fibre Channel adaptér vrátane príslušných prevodníkov |  |  |
| Dátové a video konektory | Min. 1x USB na prednom paneli  Min. 1x USB na pripojenie mobilného zariadenia typu smartfón alebo tablet pre použite manažovacej aplikácie za účelom fyzického servisovania zariadenia  Min. 2x USB porty a 1x VGA port na zadnom paneli |  |  |
| Rozširujúce sloty | Min. 2x PCIe x16 gen4 s možnosťou rozšírenia o ďalší PCIe x16 slot. |  |  |
| Bezpečnosť | Min. TPM 2.0 a Bezpečnostný tamper spínač na chassis servera |  |  |
| Napájanie | Redundantné napájacie zdroje vymeniteľné za chodu typu hot-swap |  |  |
| Ventilátory a chladenie | Vysoko-výkonné a za chodu vymeniteľné ventilátory typu hot-swap |  |  |
| Správa a monitoring | Formou vzdialenej grafickej KVM konzoly  Možnosť štartu, reštartu a vypnutia servera cez sieť LAN, nezávisle od OS  Manažment hardvéru vrátane možnosti nastavenia RAID úrovne lokálnych diskov.  Požadovaná podpora pre DMTF Redfish API.  Požadovaná možnosť vzdialenej správy aj prostredníctvom mobilných zariadení typu smartphone, PC alebo tablet pomocou HTML5.  Požadované funkcionality a prístup k aktualizáciám musia byť poskytované s časovo neobmedzeným licenčným pokrytím. |  |  |
| Predporuchová diagnostika | Predporuchová diagnostika procesorov, pamäťových modulov, RAID radičov, napájacích zdrojov, ventilátorov a HDD/SSD. |  |  |
| Záručné podmienky | 3 roky priamo od výrobcu zariadenia  Oprava poruchy najneskôr do 24h od nahlásenia, vrátane víkendov a sviatkov.  Servis bude poskytovaný v mieste inštalácie.  Nahlasovanie poruchy v režime 24x7.  Vrátane služby ponechania vadného disku zákazníkovi v prípade jeho poruchy. |  |  |

### Inštalácia HW a systémového prostredia zálohovacích serverov

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Požadované služby | * Fyzická inštalácia servera do dátovej skrine (racku) * Zapojenie kabeláže pre napájanie a sieťovú konektivitu * Konfigurácia management rozhrania servera * Aktualizácia mikrokódov servera a interných komponentov na verzie odporúčané výrobcom zariadení * Inštalácia operačného systému * Aktualizácia operačného systému na verzie používané u Objednávateľa a podľa požiadaviek zálohovacieho systému * Pripojenie servera na diskové pole určené na ukladanie záloh, kontrola funkčnosti |  |  |

## Inovácia sieťovej infraštruktúry

Implementácia novej generácie firewallov a aktívnych prvkov siete spolu s integráciou na SIEM.

### WAN smerovač

Údaje o ponúkanom zariadení/systéme:

Výrobca: <doplniť>

Model: <doplniť>

Konfigurácia: <doplniť detailnú konfiguráciu ponúkaného zariadenia/systému>

Odkaz na produktovú dokumentáciu na stránkach výrobcu (link): <doplniť link, kde je možné overiť parametre ponúkaných produktov>

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Počet portov downlink | Min. 8x 10/100/1000 Mbps |  |  |
| Počet WAN portov | Min. 2x 10/100/1000 Mbps |  |  |
| Typ uplinkov | Fixné |  |  |
| Konzolový port | USB |  |  |
| Licencia | Všetky potrebné licencie, hlavne pre podporu bezpečnostných a komunikačných funkcionalít |  |  |
| Platnosť licencie | Doživotná, v rámci zariadenia |  |  |
| Obsah licencie - security | Min. Zone-based firewall, IPsec VPN, FlexVPN, GETVPN. Základná IPsec priepustnosť min. 50 Mbps. |  |  |
| Obsah licencie - IPSec HSEC | Áno - Odomkne softvérovú blokádu v IPSEC tuneli na plnú kapacitu zariadenia |  |  |
| Softvér | Modulárny, umožňujúci licenčne odomknúť funkcionality |  |  |
| Základné protokoly a funkcie | Min. IPv4, IPv6, static routes, RIP and RIPv2, OSPF, MPLS, IPsec, L2 a L3 VPN, DES, 3DES, AES-128 or AES-256 (in CBC and GCM modes), QoS, NAT |  |  |
| HW výkon - DRAM | Min. 8 GB |  |  |
| HW výkon - Flash | Min. 4 GB |  |  |
| Priemerná kapacita smerovania na WAN pri IMIX | Min. 350 Mbps |  |  |
| Typ rozšírenej záruky | S výmenou zariadenia v nasledujúci pracovný deň v režime nahlasovania 8x5 |  |  |
| Dĺžka rozšírenej záruky | Min. 3 roky |  |  |

### Koncový prepínač s pripojením na 10GB

Údaje o ponúkanom zariadení/systéme:

Výrobca: <doplniť>

Model: <doplniť>

Konfigurácia: <doplniť detailnú konfiguráciu ponúkaného zariadenia/systému>

Odkaz na produktovú dokumentáciu na stránkach výrobcu (link): <doplniť link, kde je možné overiť parametre ponúkaných produktov>

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Počet portov downlink | Min. 48x 10/100/1000 Mbps s podporou IEEE 802.3bt type3 |  |  |
| Počet portov uplink | Min. 8x 1/10G SFP+ |  |  |
| Typ uplinkov | Modulárne |  |  |
| PoE Napájanie | AC zdroj aspoň 1100W |  |  |
| Možnosť rozšíriť o ďalší zdroj - sekundárny | Podporuje |  |  |
| Parametre sekundárneho zdroja | AC zdroj, aspoň 1100W |  |  |
| Osadenie sekundárneho zdroja | Áno, musí byť súčasťou dodávky.  Pri použití IEEE 802.3bt type3 musí byť možné týmto štandardom napájať aspoň 30 portov na zariadení |  |  |
| Licencia | S podporou L2 a základných L3 funkcionalít |  |  |
| Platnosť Licencie | Minimálne 3 roky |  |  |
| Softvér | Aktualizácie dostupné od výrobcu počas trvania subskripcie |  |  |
| Požiadavky na software | Modulárny, umožňujúci licenčne odomknúť funkcionality |  |  |
| Podpora Netflow/sFlow/IPFIX | Áno, maximálne 64 000 záznamov |  |  |
| Základné protokoly a funkcie | Layer 2, Routed Access (RIP, OSPF - 1000 routes), PBR, PIM Stub Multicast (1000 routes), PVLAN, VRRP, PBR, CDP, QoS, FHS, 802.1X, MACsec-128, SXP, IP SLA Responder,SSO, MACsec-128, Static routing |  |  |
| HW výkon - DRAM | min. 8 GB |  |  |
| HW výkon - Flash | min. 16 GB |  |  |
| HW výkon - Buffer | min. 16 MB |  |  |
| Kapacita prepínania | Minimálne 256 Gbps |  |  |
| Kapacita smerovania | Minimálne 190 Mpps |  |  |
| Minimálny počet MAC adries | 32,000 |  |  |
| Montovateľné do racku | Áno |  |  |
| Možnosť stohovania | Áno, jedna sada stohovacích káblov musí byť súčasťou dodávky |  |  |
| Kapacita prepínania v stohu | min. 460Gbps |  |  |
| Minimálna hodnota MTBF | 220 000 hodín |  |  |
| Maximálny počet VLAN | 4090 |  |  |
| Konzolový port | USB |  |  |
| Ostatné porty | USB |  |  |
| Podpora automatizácie | NETCONF, RESTCONF, YANG, PnP Agent, PnP |  |  |
| Telemetria a viditeľnosť | sampled Netflow/sFlow/IPFIX, SPAN, RSPAN |  |  |
| Podpora JUMBO rámcov | Min. 9198 bytes |  |  |
| Záručné podmienky | Doživotná limitovaná záruka |  |  |
| Možnosť zakúpiť od výrobcu rozšírenú záruku | Áno |  |  |
| Typ rozšírenej záruky | S výmenou zariadenia v nasledujúci pracovný deň v režime nahlasovania 8x5 |  |  |
| Dĺžka rozšírenej záruky | Min. 3 roky |  |  |

### Sieťový prepínač

Údaje o ponúkanom zariadení/systéme:

Výrobca: <doplniť>

Model: <doplniť>

Konfigurácia: <doplniť detailnú konfiguráciu ponúkaného zariadenia/systému>

Odkaz na produktovú dokumentáciu na stránkach výrobcu (link): <doplniť link, kde je možné overiť parametre ponúkaných produktov>

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Počet portov downlink | Min. 8 x 10/100/1000 portov |  |  |
| Počet portov uplink | Combo uplink - 2xGE SFP alebo 2xGE RJ-45 |  |  |
| Typ uplinkov | Fixné |  |  |
| PoE Napájanie | Áno, Podporuje PoE+, PoE budget min. 240W |  |  |
| Podpora perpetuálneho PoE | Podporuje |  |  |
| Požiadavky na hlučnosť | Prevedenie bez ventilátora |  |  |
| Licencia | S podporou L2 a základných L3 funkcionalít |  |  |
| Platnosť Licencie | Doživotná, v rámci zariadenia |  |  |
| Podpora Netflow/sFlow/IPFIX | Požadovaná |  |  |
| Základné protokoly a funkcie | LACP, DHCP, MVR,IEEE 802.1Q VLAN, Voice VLAN, IEEE 802.1p CoS Prioritization, RSPAN, VTP, RMON, IEEE 802.1AE MACsec, 802.1X, ARP Spoofing, ACL, Secure Boot, RIPv1, RIPv2, OSPFv1, OSPFv2, IGMP, IP Multicast, SNMPv1, SNMPv2, IEEE 802.3az, MACsec, OSPF, BGP, PBR, VRF Lite |  |  |
| HW výkon - DRAM | Min. 512 MB |  |  |
| HW výkon - Flash | Min. 128 MB |  |  |
| Kapacita prepínania | Min. 32 Gbps |  |  |
| Kapacita smerovania | Min. 17.9 mpps |  |  |
| Maximálna veľkosť prenosovej jednotky (MTU) | 9000 bytes |  |  |
| Konzolový port | 1x RJ45 console, 1x USB |  |  |
| Ostatné porty | 1x USB |  |  |
| Podpora JUMBO rámcov | max. 9198 bytes |  |  |
| Záručné podmienky | Doživotná limitovaná záruka |  |  |
| Možnosť zakúpiť od výrobcu rozšírenú záruku | Áno |  |  |
| Typ rozšírenej záruky | S výmenou zariadenia v nasledujúci pracovný deň v režime nahlasovania 8x5 |  |  |
| Dĺžka rozšírenej záruky | Min. 3 roky |  |  |

### Firewall vrátane analytických a manažment nástrojov

Údaje o ponúkanom zariadení/systéme:

Výrobca: <doplniť>

Model: <doplniť>

Konfigurácia: <doplniť detailnú konfiguráciu ponúkaného zariadenia/systému>

Odkaz na produktovú dokumentáciu na stránkach výrobcu (link): <doplniť link, kde je možné overiť parametre ponúkaných produktov>

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Forma | HW appliance s montážou do racku s veľkosťou max. 1RU.  Kompletné montážne prvky pre montáž do RACK-u.  Zariadenie vybavené dvoma zdrojmi. |  |  |
|  | Platforma postavená na HW akcelerovanej architektúre (t.j. zariadenia vybavené špecializovanými obvodmi pre spracovanie komunikácie a vybraných výpočtovo náročných funkcií). |  |  |
| Vysoká dostupnosť | HW appliance NGFW/UTM firewallu musí umožňovať režim vysokej dostupnosti (dve fyzické zariadenia rovnakého typu zapojené do funkčného clustra). |  |  |
|  | Podpora režimu vysokej dostupnosti (režim L2 cluster s využitím virtuálnych MAC adries; celý cluster sa prezentuje z pohľadu L3 ako jedno zariadenie) v režime active-active (A/A) a active-passive (A/P). Ak táto funkcia vyžaduje licenciu, tak táto musí byť súčasťou dodávky. |  |  |
| Disková kapacita | Min. 2x 220GB |  |  |
| Rozhrania na každom firewalle využiteľné pre management | Min. 2x GE RJ45 |  |  |
| Rozhrania na každom firewalle využiteľné pre spracovanie komunikácie | Min. 2x 10 GE SFP+, 10x GE RJ45, 8x GE SFP |  |  |
| Podpora VLAN | Min. 4000 |  |  |
|  | Podpora LACP |  |  |
| Počet FW pravidel | Min. 8000 |  |  |
|  | Možnosť definície FW pravidel v tzv. NGFW režime, tj. súčasťou základnej definície FW pravidla je min. zdrojové a cieľové rozhranie, zdrojová a cieľová adresa, služba, čas, aplikácia, používateľ, kategórie URL filteringu. |  |  |
| Celková priepustnosť firewallu | Min. 30 Gbps (pri paketoch s veľkosťou 1518B) |  |  |
| Latencia firewallu | Nepresahuje 3 μs |  |  |
| Počet nových spojení za sekundu (setup-rate) | Min. 250 000 |  |  |
| Celkový počet súčasných TCP spojení firewallu | Min. 3 500 000 |  |  |
| PPS (počet spracovaných paketov za 1 sekundu) | Min. 25 000 000 |  |  |
| Funkcia detekcie aplikácií na L7 (Application Control) | Áno |  |  |
| Detekcia známych aplikácií na základe signatúr | Áno, min. 2 000 preddefinovaných aplikácií/signatúr, pre cloud aplikácie - minimálne Facebook, Dropbox, Flickr, Google Apps, iCloud, LinkedIn) - sa požaduje funkcionalita blokovania upload/download súborov, blokovanie hier, blokovanie login, atď.  Pre aplikácie je požadované : povolenie, blokovanie, monitorovanie a možnosť obmedzenia šírky pásma pre danú aplikáciu. |  |  |
|  | Priepustnosť funkcie Application Control vrátane logovania (merané s HTTP response) min. 6,8 Gbps  Podpora použitia Application control aj formou profilov priradených k pravidlám. |  |  |
| Funkcie detekcie a zamedzenia narušení (IPS/IDS) | Počet rozpoznávaných hrozieb (signatúr) definovaných výrobcom min. 11 000.  Priepustnosť funkcie IPS vrátane logovania min. 4,7 Gbps. |  |  |
|  | Funkcia IPS sa konfiguruje v rámci IPS profilov, ktoré sú následne priradené konkrétnym FW pravidlám. |  |  |
|  | Možnosť tvorby vlastných signatúr pre aplikačnú kontrolu a IPS. |  |  |
| Funkcie antivírovej kontroly | Ochrana pred škodlivým kódom, vrátane ochrany pred polymorfným kódom. |  |  |
|  | AV kontrola s možnosťou rozšírenia o inšpekciu tzv. sandbox technikou. |  |  |
|  | Podpora služby výrobcu umožňujúca detegovať malware, ktorý bol objavený v dobe od poslednej aktualizácie AV signatúrovej databázy pomocou priebežne aktualizovanej databázy hash-ov. |  |  |
|  | Podpora funkcie odstránenia aktívneho obsahu z dokumentov kancelárskych aplikácií – AV engine na firewalle v reálnom čase odstráni aktívny obsah z dokumentu, pričom tento zostáva v pôvodnom formáte, ale sú z neho odstránené všetky aktívne prvky. |  |  |
| Priepustnosť FW pri zapnutí IPS, Application Control, Antivirus, Web Filtering a zapnutým logovaním | Min. 3 Gbps |  |  |
| Podpora SSL dešifrovania/SSL inšpekcie | Min. 3,8 Gbps (HTTPS prevádzka, merané v kombinácii s IPS kontrolou) |  |  |
| Funkcia DNS filtra | Možnosť blokovať DNS dotazy na základe príslušnosti k URL kategórii. |  |  |
|  | Možnosť definovať vlastný tzv. blacklist domén. |  |  |
|  | Možnosť presmerovať komunikáciu so zakázanými doménami na vlastný portál/URL. |  |  |
|  | Podpora funkcie explicit proxy s možnosťou aktivovania požadovaných ochranných profilov (AV, IPS, AppCtrl, DLP, Web Filtering) a podpora transparentného overovania používateľov voči MS AD protokolom Kerberos. |  |  |
|  | Funkcia transparentného overovania používateľov pomocou domény (MS Active Directory) vrátane podpory autentifikácie používateľov na terminálovom serveri. |  |  |
| Podpora SSL VPN | Priepustnosť SSL VPN min. 2,2 Gbps. |  |  |
|  | Podpora IPSEC VPN v režime site-2-site aj client-2-site. |  |  |
|  | Priepustnosť IPSEC VPN (AES256-SHA256) min. 20 Gbps. |  |  |
| Správa | Podpora virtualizácie FW na danom HW. Každý virtuálny FW musí byť plnohodnotné riešenie vrátane oddeleného managementu účtov, objektov, politík, smerovania a pod. |  |  |
|  | FW cluster je možné plnohodnotne spravovať pomocou lokálneho GUI a CLI, bez nutnosti inštalovať klienta na koncovú (management) stanicu. |  |  |
|  | Jedno manažment rozhranie pre celý cluster, akákoľvek zmena je medzi jednotlivými uzlami klastra synchronizovaná automaticky. |  |  |
|  | Podpora SNMP vrátane SMPB MIB súboru dodávaného výrobcom, možnosť začlenenia do existujúceho systému dohľadu siete. |  |  |
|  | Požaduje sa certifikácia ICSA Labs alebo ekvivalent minimálne pre Firewall. |  |  |
|  | Možnosť automatizácie na základe udalostí, ktoré je Firewall schopný zaznamenať. |  |  |
|  | Možnosť kombinovať akcie pre automatizačné pravidlá - min. webhook s definovateľnými parametrami, CLI script, Email, MS-TEAMS notifikácia, Slack notifikácia, Karanténa na základe IP, MAC adresy. |  |  |
|  | Možnosť použitia dynamických vstupných parametrov v rámci automatizačných pravidiel – min. schopnosť parsovat vstupy z logov a z predchádzajúcich vykonaných akcií. |  |  |
|  | Podpora otvoreného API pre ďalšie možnosti integrácie. |  |  |
| Záručné podmienky | Podpora a údržba pre HW zariadenie a softvér musí zahŕňať upgrade a aktuálne opravné balíky (fixies, patch).  Denné online aktualizácie údajov (databáz) pre použité funkcionality |  |  |
|  | Softvérové licencie riešenia vrátane trojročnej údržby a podpory podľa špecifikácie komponentov riešenia. |  |  |

### UPS 5000VA

Údaje o ponúkanom zariadení/systéme:

Výrobca: <doplniť>

Model: <doplniť>

Konfigurácia: <doplniť detailnú konfiguráciu ponúkaného zariadenia/systému>

Odkaz na produktovú dokumentáciu na stránkach výrobcu (link): <doplniť link, kde je možné overiť parametre ponúkaných produktov>

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Výkon | Min. UPS 4500W / 5kVA/ 230V |  |  |
|  | Montáž do racku, veľkosť maximálne 6U |  |  |
|  | Poskytuje čistý sínusový výstup s kompenzáciou účinníka (PFC) |  |  |
|  | Bypass manuálny aj automatický |  |  |
| Vstupné napätie | 230V AC, 1-fázové |  |  |
| Doba zálohovania | Doba zálohovania pri plnom výkone minimálne 12 minút |  |  |
| Rozšírenie | Možnosť rozšírenia o externé batériové kabinety |  |  |
| Pripojenie | Minimálne 2x 1-fázová rozvodná jednotka PDU s max. prúdom 32A  PDU nesmie obsadzovať pozície pre servery a iné zariadenia (prevedenie 0U) |  |  |
| Počet napájacích konektorov | Minimálne 36 konektorov C13 pre každé PDU  Minimálne 6 konektorov C19 pre každé PDU |  |  |
| Komunikačné rozhranie minimálne | 10/100 Base-T |  |  |
|  | RJ-45 Serial |  |  |
|  | Smart-Slot |  |  |
|  | USB |  |  |
| Ostatné | Čidlo snímača teploty |  |  |

### Káble CAT 5E UTP

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Patchcordy pre pripojenie dodávaných sieťových zariadení | Kategória minimálne 5E  Typ kábla UTP  Koncovky RJ-45 |  |  |

### Vypracovanie návrhu riešenia sieťovej infraštruktúry

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Vypracovanie návrhu riešenia sieťovej infraštruktúry | **Dokument s minimálnym obsahom:**  Popis navrhnutých služieb a komponentov  Návrh fyzickej architektúry  Návrh logickej topológie  Návrh segmentácie siete, adresný plán  Návrh riešenia UPS  Požiadavky na komunikáciu – definícia sieťových prestupov, atď.  Požiadavky na infraštruktúrne služby (Active Directory, 2FA a ďalšie)  Popis konfigurácie jednotlivých funkcií, služieb a komponentov  Návrh migračného postupu  Návrh testovacích scenárov |  |  |

### Konfigurácia aktívnych prvkov sieťovej infraštruktúry

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Konfigurácia aktívnych prvkov | Inštalácia do rack-u  Pripojenie kabeláže na základe návrhu  Základná konfigurácia manažment portov  Implementácia manažment rozhrania  Pripojenie sieťových prvkov do manažmentu  Konfigurácia WAN routrov, switchov a FW |  |  |

### Overovanie a ladenie sieťovej infraštruktúry

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Overovanie a ladenie sieťovej infraštruktúry | Kontrola dostupnosti na prístupovej vrstve siete  Kontrola bezpečnostných pravidiel na FW  Kontrola a ladenie routingu s ISP  Kontrola core vrstvy siete a dostupnosti jednotlivých služieb ako nevyhnutného základu pre následnú implementáciu ďalších systémov  Testy na základe odsúhlasených testovacích scenárov |  |  |

### Vypracovanie dokumentácie riešenia sieťovej infraštruktúry

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Vypracovanie dokumentácie riešenia sieťovej infraštruktúry | Dokumentácia skutočného vyhotovenia – fyzická topológia, logická topológia, segmentácia siete, adresný plán  Doplnenie skutočného umiestnenia podporných sieťových služieb – NTP, DNS, AD, DHCP, atď.  Dokumentácia skutočného stavu k jednotlivým vrstvám siete – minimálne L1, L2, L3 |  |  |

### Zaškolenie administrátorov sieťovej infraštruktúry

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Zaškolenie administrátorov sieťovej infraštruktúry | Zaškolenie obslužného personálu na kompletný rozsah dodaného HW a SW |  |  |

### Montáž, konfigurácia, oživenie UPS

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Montáž, konfigurácia, oživenie UPS | Inštalácia do rack-u  Inštalácia prívodného napájania  Inštalácia PDU  Konfigurácia manažmentu  Inštalácia dodaných doplnkových komponentov  Test funkčnosti  Bezvýpadková inštalácia |  |  |

## Prevencia úniku dát

V súčasnosti nie je implementované technické riešenie pre zabránenie úniku dát z používateľských počítačov. Implementáciou softvéru pre prevenciu úniku dát z používateľských počítačov bude možné zabezpečiť dôležité a citlivé údaje pred únikom.

### Softvér pre prevenciu úniku dát z používateľských počítačov

Údaje o ponúkanom zariadení/systéme:

Výrobca: <doplniť>

Model: <doplniť>

Konfigurácia: <doplniť detailnú konfiguráciu ponúkaného zariadenia/systému>

Odkaz na produktovú dokumentáciu na stránkach výrobcu (link): <doplniť link, kde je možné overiť parametre ponúkaných produktov>

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Základné požiadavky | Riešenie musí mať možnosť centralizovanej správy cez jednotnú vzdialenú konzolu. Vzdialená konzola musí umožňovať správu cieľových zariadení, koncových bodov, pravidiel a reportov. |  |  |
|  | Riešenie má mať zabudované pravidlá pre viac priemyselných odvetví a lokalít, musí sa dať do nich vstúpiť, využívať ich a aplikovať ich súčasne. |  |  |
|  | Riešenie musí umožniť konfigurovať bodovanie vážnosti incidentov. |  |  |
|  | Riešenie musí umožniť vyňať a preveriť obsah textu súborov a príloh. |  |  |
|  | Riešenie musí umožniť preveriť metadáta v súboroch v rámci preverovania uloženého obsahu. |  |  |
|  | Riešenie musí podporovať detekciu citlivých dát na základe podobnosti s určitým iným druhom dát pomocou strojového učenia sa. Napríklad detekcia novej obchodnej zmluvy na základe podobnosti s už označenými obchodnými zmluvami. |  |  |
|  | Riešenie musí vedieť rekurzívne preveriť obsah komprimovaných archívov (napr. ZIP, TAR, RAR) a detegovať voči odtlačkom obsahu. |  |  |
|  | Riešenie musí vedieť detegovať na základe typu dokumentu, aj keď odosielateľ zmenil príponu súboru. |  |  |
|  | Riešenie musí umožňovať fingerprinting neštruktúrovaných ako aj štruktúrovaných dát. |  |  |
|  | Riešenie musí byť schopné čítať text z  obrázkov a PDF dokumentov uložených ako obrázky. |  |  |
|  | Riešenie musí vedieť automaticky upozorniť odosielateľov alebo ich manažérov, keď dôjde k porušeniu politiky. |  |  |
|  | Riešenie musí vedieť poskytnúť automatické notifikácie incidentov rôznym útvarom, ako napr. právnemu a útvaru informačnej bezpečnosti. |  |  |
|  | Riešenie musí obsahovať workflow s funkcionalitou automatického sledovania nápravy incidentu (napr. kódy stavu, atribúty, priradenie do fronty, závažnosť incidentu a pod.). |  |  |
|  | Riešenie bude podporovať pripojenie a dohľad minimálne nasledovných monitorovaných systémov - pracovné stanice s OS Windows a MAC OS, Linux, Doménové radiče, MS Exchange, atď. |  |  |
|  | Riešenie musí umožniť vytvoriť oddelené roly pre technickú správu serverov, správu používateľov, vytváranie a zmeny politiky, nápravu incidentov, zobrazovanie incidentov pre dáta v pokoji, v pohybe, alebo v koncovom bode. |  |  |
|  | Riešenie musí mať kontrolu autentifikácie používateľa voči externej databáze, napr. Active Directory. |  |  |
|  | Všetky systémové moduly musia byť riadené prostredníctvom centrálneho UI. |  |  |
|  | Databáza backendu by sa mala zdieľať s ostatnými súčasťami riešenia (s ochranou webu). |  |  |
|  | Riešenie musí poskytovať integráciu s e-mail encryption bránou. |  |  |
|  | Riešenie musí podporovať systém VMware, Microsoft Hyper-V, CITRIX. |  |  |
|  | Riešenie musí podporovať integráciu s  riešením pre archiváciu emailov. |  |  |
|  | Riešenie musí vedieť analyzovať prenos a reportovať incidenty v reálnom čase aj pri vysokom zaťažení. |  |  |
|  | Riešenie musí poskytnúť podrobnosti v súvislosti s lokalitou a webovou stránkou na resolvovanie / klasifikáciu destinácie prenosu HTTP/S (nie len IP adresy). |  |  |
|  | Riešenie musí byť schopné odhaliť viacnásobné incidenty v priebehu času (napr. pomalý únik, ktorý v priebehu času prejde do straty dôležitých údajov). |  |  |
|  | Riešenie musí umožňovať uplatňovať (monitorovať a blokovať) politiky pri ukladaní dát do cloudových služieb (minimálne pre služby Office 365). |  |  |
|  | Riešenie musí podporovať spoluprácu s externými nástrojmi na tagovanie – musí byť možné čítať a zapisovať tagy na súbory pomocou ľubovoľného tagovacieho nástroja, napr. MIP, AIP, DocTag, Titus atď. |  |  |
|  | Navrhované riešenie musí odhaliť pokusy používateľa o zaslanie dôverných údajov prostredníctvom internetových protokolov, napríklad e-mailom, webmailom (Yahoo!, Gmail), IM alebo FTP, aj keď je koncový bod odpojený od podnikovej siete. Umožňovať automatické šifrovanie citlivých dát pri uložení na USB disk. |  |  |
|  | Riešenie má mať zabudované pravidlá pre viac priemyselných odvetví a lokalít, musí sa dať do nich vstúpiť, využívať ich a aplikovať ich súčasne. |  |  |
|  | Riešenie musí mať možnosť zamedzovať vytváraniu kópií na prenosné médiá. |  |  |
|  | Riešenie musí vedieť aplikovať rôzne politiky pre rôznych koncových používateľov alebo skupiny používateľov, a uplatniť rôzne politiky, aj keď sú títo používatelia nahlásení na ten istý koncový počítač. |  |  |
|  | Riešenie musí byť schopné označiť rizikových používateľov na základe analýzy ich chovania. Malo by disponovať predpripravenými politikami a scenármi, ktoré rizikové chovanie detegujú. |  |  |
|  | Riešenie musí umožňovať okamžité vyhľadávanie citlivých dát na všetkých koncových staniciach zahrnutých do riešenia– možnosť na základe vzorky napr. dokumentu, textu, alebo dát z databázovej tabuľky vyhľadať kde (na ktorom konkrétnom koncovom bode) sa nachádzajú fragmenty daného dokumentu, textu nebo dát a to v rámci jednotiek hodín pre celú organizáciu. |  |  |
|  | Riešenie musí mať možnosť pre administrátorov, aby na diaľku zablokovali koncový bod. |  |  |
|  | Riešenie musí vedieť presadiť rôzne politiky, ak je k dôveryhodnej podnikovej sieti pripojený koncový bod a ak je pripojený k nedôveryhodnej verejnej sieti (letisko, kaviareň, domáca sieť, atď.). |  |  |
|  | Riešenie musí plne podporovať integráciu so systémami SIEM. |  |  |
|  | Riešenie musí plne podporovať ukladanie forenzných dát aj priamo na manažment serveri – musí podporovať a poskytovať možnosť manuálneho overenia závažnosti DLP incidentov využitím forenzných dát uložených na manažment serveri. |  |  |
|  | Riešenie má mať detekciu údajov založenú na agentoch na zariadeniach koncových používateľov. |  |  |
|  | Riešenie pre koncové zariadenie má podporovať automatickú aktualizáciu agentov a zmeny v politike bez nástrojov tretej strany. |  |  |
|  | Agent na koncovom bode musí podporovať všetky podporované Windows OS a Mac OS, Linux. |  |  |
| Používateľské požiadavky | Riešenie musí umožňovať definovať typ a rozsah prístupu podľa rolí – minimálne systémový administrátor, administrátor, audítor, používateľ, prípadne rolu s rozsahom prístupov, ktoré sú kombináciou vyššie uvedených rolí. |  |  |
| Reporting | Riešenie musí vedieť údaje  v reportoch exportovať do formátov ako PDF alebo HTML, XLS. |  |  |
|  | Riešenie musí umožniť zdieľať reporty na základe role. |  |  |
|  | Riešenie musí vedieť zoskupiť jednotlivé incidenty do skupín podľa zdroja, alebo povahy incidentu a vytvoriť informáciu o rizikových užívateľoch za definovaný čas. |  |  |
|  | Riešenie musí poskytovať preddefinované reporty s možnosťou ich parametrizácie, ako aj s možnosťou vytvárať reporty na základe aktuálnych požiadaviek. |  |  |
|  | Riešenie musí umožňovať tlač ľubovoľného reportu. |  |  |
|  | Riešenie musí byť flexibilné a musí generovať reporty na požiadanie alebo v periodických intervaloch. |  |  |
| Kapacitné požiadavky | Riešenie musí byť dimenzované na 150 používateľov v doméne. |  |  |
|  | Riešenie musí obsahovať vlastnú databázu, ak ju pre svoju činnosť vyžaduje. |  |  |
|  | Riešenie musí umožňovať zálohovanie aplikáciou, dodávanou v rámci projektu „Centrálny systém zálohovania dát“. |  |  |
|  | Riešenie musí umožniť, aby bola v budúcnosti zabezpečená jeho vysoká dostupnosť (HA) / musí podporovať vysokú dostupnosť- |  |  |
|  | Riešenie musí poskytovať intuitívne používateľské rozhranie a centralizovanú správu. |  |  |
| Bezpečnostné požiadavky | Riešenie musí podporovať autentifikáciu a riadenie prístupov založené na jednoznačnom identifikátore entity. |  |  |
|  | Riešenie musí podporovať využitie silnej (viacfaktorovej) autentifikácie. |  |  |
| Podpora a údržba | Podpora a údržba softvéru musí zahŕňať upgrade a aktuálne opravné balíky (fixies, patch). |  |  |
|  | Softvérové licencie riešenia vrátane trojročnej údržby a podpory podľa špecifikácie komponentov riešenia. |  |  |

### Vypracovanie návrhu riešenia systému pre prevenciu úniku dát z používateľských počítačov

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Vypracovanie návrhu riešenia | Popis funkcionalít, ktoré sa budú používať  Používané služby a komponenty  Návrh architektúry riešenia  Požiadavky na licencie – licenčný model, možnosti rozšírenia riešenia  Hardvérové požiadavky  Softvérové požiadavky  Návrh klasifikácie dát a dokumentov  Požiadavky na integráciu s infraštruktúrnymi službami (Active Directory, a ďalšie)  Popis konfigurácie jednotlivých funkcií, služieb a komponentov  Zálohovanie a obnova systému, konfigurácie a dáta  Návrh testovacích scenárov |  |  |

### Konfigurácia softvéru pre prevenciu úniku dát z používateľských počítačov

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Konfigurácia softvéru | Inštalácia a konfigurácia komponentov.  Integrácia s existujúcou, resp. dodávanou infraštruktúrou - AD, mail server, web brána, atď.  Definovanie prístupov, politík.  Konfigurácia správy a dohľadu.  Vytvorenie používateľov a rolí.  Vytvorenie korelačných pravidiel-politík podľa najnovších znalostí „dobrej praxe“  Nastavenie preddefinovaných politík, vlastných politík.  Nastavenie OCR.  Nasadenie riešenia pre 150 používateľov).  Implementácia pravidiel pre discovery.  Implementácia nástroja pre automatizovanie klasifikácie dokumentov. |  |  |

### Overovanie a ladenie systému pre prevenciu úniku dát z používateľských počítačov

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Overovanie a ladenie | Skúšobná prevádzka v trvaní 3 mesiace a vykonanie vopred odsúhlasených akceptačných testov:  Detailné monitorovanie prevádzkových hodnôt a úprava parametrov.  Ladenie výkonu riešenia.  Ladenie False positive hlásení.  Analýza výstupov analytických prvkov a ich ladenie.  Testovanie. |  |  |

### Vypracovanie dokumentácie riešenia systému pre prevenciu úniku dát z používateľských počítačov

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Vypracovanie dokumentácie riešenia | Vypracovanie a dodanie projektovej dokumentácie v rozsahu: dokumentácia výrobcu, technická dokumentácia popisujúca skutočné vyhotovenie, používateľská príručka.  **Minimálne požiadavky na technickú dokumentáciu:**  Popis funkcionalít, ktoré sa používajú.  Používané služby a komponenty.  Popis architektúry riešenia a obrazová schéma.  Používané licencie.  Popis hardvérovej konfigurácie.  Zoznam nainštalovaného softvéru.  Popis používaných infraštruktúrnych služieb (Active Directory, group policy a ďalšie).  Popis konfigurácie jednotlivých funkcií, služieb a komponentov.  Príklady tvorby a aktivácie vlastných politík  Popis zálohovania a obnovy riešenia, konfigurácie a dát. |  |  |

### Zaškolenie administrátorov systému pre prevenciu úniku dát z používateľských počítačov

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Zaškolenie administrátorov | Školenie na jednotlivé roly určené pre podporu prevádzky aplikácie. |  |  |

## Proxy server (webová brána pre prístup z internej siete do Internetu)

Webová brána umožní aplikovať politiky ochrany pre komunikáciu z a do internetu, ako aj detekciu škodlivého kódu. Rovnako tento systém umožní nastaviť a vynucovať pravidlá pre prístup používateľov do internetu.

### Proxy server (webová brána)

Riešenie musí byť vysoko dostupné, čiže predmetom dodávky budú 2 ks HW appliances.

Údaje o ponúkanom zariadení/systéme:

Výrobca: <doplniť>

Model: <doplniť>

Konfigurácia: <doplniť detailnú konfiguráciu ponúkaného zariadenia/systému>

Odkaz na produktovú dokumentáciu na stránkach výrobcu (link): <doplniť link, kde je možné overiť parametre ponúkaných produktov>

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Architektúra, konektivita | Riešenie musí byť dostupné v rôznych spôsoboch nasadeniach. Musí podporovať nasadenie HW zariadenia (HW appliance), virtuálneho zariadenia (virtual appliance) a softvéru. |  |  |
|  | Riešenie musí byť schopné zvládnuť riadenie niekoľkých pripojení. V prípade potreby musia byť k dispozícii bezplatné inštancie virtuálneho zariadenia (virtual appliance). |  |  |
|  | Riešenie musí podporovať možnosti mobilného zabezpečenia umožňujúceho ochranu používateľov, keď sa nachádzajú mimo hlavnej siete. |  |  |
|  | V prípade, že HW zariadenie zlyhá, musí byť riešenie schopné kontrolovať všetku komunikáciu cez cloud app (konfigurácia funkcionality nie je predmetom projektu). |  |  |
|  | Používatelia, umiestnení mimo hlavnej siete, musia byť riadení rovnakými zásadami, ako keby boli vo vnútornej sieti. |  |  |
|  | Architektúra by mala poskytovať funkcie na správu a riadenie spotreby šírky pásma, aby sa zabezpečila dostupnosť pre kritické aplikácie alebo protokoly. |  |  |
| Výkonnosť | Riešenie musí byť schopné zvládnuť minimálne 400 Mb/s prenosmi HTTP a HTTPS. |  |  |
| Hardware | HW appliance |  |  |
| Konektivita | min. 4x 10/100/1000 NIC |  |  |
| Manažment | Riešenie musí byť spravované prostredníctvom centrálnej webovej konzoly. |  |  |
|  | Systém riadenia by mal poskytovať možnosti monitorovania používateľov v reálnom čase, tzn. zahŕňať informácie o totožnosti používateľa a podrobnosti cieľovej adresy URL. |  |  |
|  | Systém riadenia by mal poskytovať všetky prvky politiky na jednej obrazovke alebo karte. |  |  |
|  | Riešenie musí podporovať viac administratívnych účtov založených na rolách, ktoré poskytujú možnosti a obmedzenia podrobnej správy. |  |  |
|  | Riešenie musí podporovať centralizovanú správu a vykazovanie na viacerých lokalitách vrátane vzdialených používateľov, ktorí sa nenachádzajú v žiadnej z interných sietí. |  |  |
|  | Riešenie musí podporovať administračné roly „iba na vytváranie prehľadov“, ktoré jednotlivcom alebo skupinám umožňujú prístup k údajom prehľadov o určených používateľoch alebo skupinách. |  |  |
| Reporting | Riešenie musí poskytovať preddefinované zostavy pre používateľov, skupiny alebo umiestnenia o správaní, trendoch atď. |  |  |
|  | Riešenie musí umožňovať spojiť prevenciu zaznamenaných hrozieb, kontrolu webového obsahu a prevenciu straty údajov s adresou IP, menom používateľa a kategóriou prístupu na webovú stránku. |  |  |
|  | Riešenie nesmie mať žiadne systémové časové ani veľkostné obmedzenie pre ukladanie protokolov. Úložisko musí poskytovať dostatočnú kapacitu na minimálne 3 roky. |  |  |
|  | Riešenie musí obsahovať podrobné informácie o aktivite používateľov vrátane úplného protokolovania adries URL a zobrazenia primárneho umiestnenia a všetkých prepojených stránok. |  |  |
|  | Riešenie musí podporovať anonymné hlásenie správania a aktivít s odstránením alebo maskovaním citlivých osobných údajov. |  |  |
|  | Riešenie musí podporovať zobrazenia traffic-u v reálnom čase pre okamžité riešenie problémov. |  |  |
|  | Riešenie musí umožniť nahlásiť každú použitú cloudovú aplikáciu a nahlásiť rizikové skóre danej aplikácie s popisom (min. 3 000 aplikácií). |  |  |
|  | Riešenie musí byť schopné identifikovať a hlásiť konkrétneho používateľského agenta a operačný systém použitý na prehliadanie. |  |  |
|  | Ak počítač prehľadáva web mimo sieť organizácie, protokoly musia byť synchronizované s ostatnými protokolmi prehľadávania on-premises. |  |  |
| Manažment hrozieb | Riešenie musí obsahovať vopred vyplnený zoznam adries URL a webových stránok, o ktorých je známe, že boli napadnuté alebo infikované. |  |  |
|  | Riešenie musí byť schopné identifikovať a zablokovať známy malvér bez ohľadu na prichádzajúci sieťový port. |  |  |
|  | Riešenie musí detegovať a blokovať odchádzajúcu komunikáciu škodlivého softvéru typu Botnet a Trojan z infikovaných systémov. Systém sa musí prihlásiť a poskytnúť podrobné informácie o pôvodnom systéme dostatočné na to, aby umožnil identifikáciu infikovaných jednotiek na mitigáciu. |  |  |
|  | Riešenie musí byť schopné kontrolovať prenos šifrovaný pomocou TLS na prítomnosť škodlivého softvéru a iných hrozieb. |  |  |
|  | Riešenie musí chrániť pred známymi binárnymi spustiteľnými súbormi, exploitmi založenými na skriptoch a kódoch alebo skriptmi vstupujúcimi do siete. |  |  |
|  | Riešenie musí byť schopné blokovať zoznam webovských adries (Uniform Resource Locators) a stránok odkazujúcich na stránky infikované malvérom (aj keď samotný web nie je infikovaný). |  |  |
|  | Riešenie musí byť schopné dynamicky blokovať infikovanú legitímnu webovú stránku a odblokovať dočasné obmedzenie stránky, ak bola hrozba odstránená nezávisle od zabudovanej databázy URL. Toto musí platiť aj pre prenos TLS. |  |  |
|  | Riešenie musí mať možnosť posielať dešifrovanú TLS traffic do analyzátorov tretích strán. |  |  |
|  | Riešenie musí obsahovať možnosť odosielať dáta do sandboxu (lokálneho alebo cloudového). |  |  |
| Kontrola webového obsahu | Riešenie musí obsahovať vopred vyplnený zoznam adries URL (najmenej 100 kategórií adries URL). |  |  |
|  | Riešenie musí byť schopné kontrolovať porušenie pravidiel v prenosoch dát šifrovaných pomocou TLS. |  |  |
|  | Riešenie musí byť schopné dynamicky klasifikovať webové stránky a webové prvky tak, aby umožnilo vynútenie politiky na webových stránkach, ktoré nie sú obsiahnuté v databáze URL. |  |  |
|  | Riešenie musí byť schopné prepísať kategóriu uvedenú v databáze URL aktualizovanou kategóriou určenou mechanizmom dynamickej klasifikácie, aby sa zabezpečilo presné vynucovanie politiky. |  |  |
|  | Riešenie musí byť schopné poskytnúť špecifické kontrolné prvky pre rôzne bežné protokoly a aplikácie, ktoré je možno použiť ako vektor útoku. |  |  |
|  | Riešenie musí byť schopné identifikovať a blokovať konkrétne aplikácie bez ohľadu na používaný port TCP. |  |  |
| Klientsky softvér | Riešenie musí obsahovať licenčné pokrytie pre 150 používateľov. |  |  |
|  | Klienti koncových bodov musia byť v budúcnosti schopní vynútiť filtrovanie webu, keď je zariadenie mimo kancelárskej siete bez VPN. |  |  |
| Manažment | Prostredníctvom centrálnej webovej konzoly |  |  |
|  | Súčasťou dodávky musia byť aj licencie tretích strán, ak sú potrebné |  |  |
| Záručné podmienky | Podpora výrobcu - min. 3 roky, vrátane licencií a aktualizácií |  |  |
|  | Podpora výrobcu je požadovaná v časovom pokrytí 24x7 (HW záruka výrobcu) v mieste inštalácie |  |  |
|  | HW záruka výrobcu so servisom najbližší pracovný deň v mieste inštalácie (okamžitá výmena - poskytnutie náhradného hardvéru nasledujúci pracovný deň po uznaní chyby support-om výrobcu). |  |  |

### Vypracovanie návrhu riešenia proxy serverov

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Vypracovanie návrhu riešenia | Popis funkcionalít, ktoré sa budú používať.  Používané služby a komponenty.  Návrh architektúry riešenia.  Požiadavky na licencie – licenčný model, možnosti rozšírenia riešenia.  Hardvérové požiadavky.  Softvérové požiadavky.  Návrh politík.  Požiadavky na integráciu s infraštruktúrnymi službami (Active Directory, ďalšie).  Popis konfigurácie jednotlivých funkcií, služieb a komponentov.  Zálohovanie a obnova systému, konfigurácie a dáta.  Návrh testovacích scenárov. |  |  |

### Konfigurácia proxy serverov

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Konfigurácia softvéru | Inicializačná inštalácia (inštalácia do rack-u, oživenie, inštalácia upgrade/firmware).  Pripojenie do siete.  Základná konfigurácia zariadenia – integrácia s infraštruktúrnymi službami – napr. NTP, DNS.  Konfigurácia a zapojenie do centrálneho manažmentu.  Integrácia s AD, LDAP.  Konfigurácia politík podľa návrhu.  Integrácia na systém zálohovania a integrácia so systémom SIEM.  Presmerovanie prevádzky (explicitne/transparentne). |  |  |

### Overovanie a ladenie proxy serverov

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Overovanie a ladenie | Optimalizácia politík a ladenie (v období min. 3 mesiace od odovzdania)  Testovanie podľa vopred odsúhlasených testovacích scenárov |  |  |

### Vypracovanie dokumentácie riešenia proxy serverov

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Vypracovanie dokumentácie riešenia | Vypracovanie a dodanie projektovej dokumentácie v rozsahu: dokumentácia výrobcu, technická dokumentácia popisujúca skutočné vyhotovenie, používateľská príručka.  **Minimálne požiadavky na technickú dokumentáciu:**  Popis funkcionalít, ktoré sa používajú.  Používané služby a komponenty.  Popis architektúry riešenia a obrazová schéma.  Používané licencie.  Popis hardvérovej konfigurácie.  Zoznam nainštalovaného softvéru.  Popis konfigurácie jednotlivých funkcií, služieb a komponentov.  Popis zálohovania a obnovy riešenia, konfigurácie a dát. |  |  |

### Zaškolenie administrátorov proxy serverov

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Zaškolenie administrátorov | Školenie na jednotlivé roly pre podporu prevádzky aplikácie v trvaní min. 4 hodiny, v priestoroch obstarávateľa |  |  |

## SIEM systém novej verzie

Aktuálne je implementovaný SIEM systém, avšak je len limitovane nasadený (na limitovaný počet systémov, je len na centralizované systémy a s limitovanými funkciami - ide o open source verziu). Požadovaný SIEM umožní monitoring IS, platforiem, aplikácií a používateľských činností a aktivít, sledovanie zraniteľností, ako aj log management a podporu riadenia incidentov vrátane prepojenia na systém na spracovanie tiketov. Systém bude implementovaný na dodávanej virtualizačnej platforme.

### SIEM riešenie

Údaje o ponúkanom zariadení/systéme:

Výrobca: <doplniť>

Model: <doplniť>

Konfigurácia: <doplniť detailnú konfiguráciu ponúkaného zariadenia/systému>

Odkaz na produktovú dokumentáciu na stránkach výrobcu (link): <doplniť link, kde je možné overiť parametre ponúkaných produktov>

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Parameter riešenia SIEM - výkon | Min. 250 Events per Second |  |  |
| Funkčné požiadavky | Riešenie musí poskytovať centrálnu webovú konzolu, z ktorej je možné spravovať celé riešenie. |  |  |
|  | Ponúkané riešenie musí poskytovať webové používateľské rozhranie, ktoré by nemalo byť založené na technológiách Java, Flash alebo na báze tučného klienta. |  |  |
|  | Riešenie nesmie byť licenčne obmedzované počtom zdrojov udalostí (logov). |  |  |
|  | Riešenie nesmie byť licenčne obmedzené počtom používaných korelačných pravidiel. |  |  |
|  | Riešenie nesmie byť licenčne obmedzené počtom existujúcich reportov alebo počtom reportov, ktoré je možné si vytvoriť. |  |  |
|  | Riešenie musí obsahovať predpripravené (out-of-box) analytické a korelačné pravidlá, ktoré je možné používať ihneď po inštalácii. |  |  |
|  | Riešenie musí umožňovať použitie šifrovanej komunikácie medzi riešením a zdrojmi udalostí (logov). |  |  |
|  | Riešenie musí podporovať prácu s internými prekrývajúcimi sa rozsahmi adries spolu so sieťovými tokmi, udalosťami a zariadeniami v sieti. |  |  |
|  | Riešenie musí podporovať agregáciu udalostí z udalostí aj podľa položiek, ktoré nie sú zahrnuté v riešení priamo od výrobcu, tzn. umožňuje agregáciu pomocou vlastných pridaných položiek. |  |  |
|  | Riešenie musí umožňovať definíciu používateľských oprávnení tak, aby bola možnosť oddelenia prístupu jednotlivých administrátorov k jednotlivým zariadeniam, ich skupinám alebo sieťovým segmentom. |  |  |
|  | Riešenie musí podporovať monitoring sieťovej komunikácie v rámci virtualizovaného prostredia. |  |  |
|  | Riešenie musí obsahovať vstavaný mechanizmus na klasifikáciu systémov podľa typu do kategórií, t. j. identifikáciu zdrojov logov. |  |  |
|  | Riešenie musí podporovať schopnosť korelovať dáta o udalostiach so statickými a dynamickými zoznamami pre možnosť vytvárať napríklad zoznamy povolených zariadení a naopak. |  |  |
|  | Riešenie musí umožňovať rozšírenie výberov o používateľské položky z obsahu logov. |  |  |
|  | Riešenie musí vykonávať tzv. Near-real-time analýzu udalostí, teda v momente príchodu udalosti do riešenia bude udalosť testovaná korelačnými pravidlami. |  |  |
|  | Riešenie musí umožňovať vykonávať analýzu dlhodobých trendov, ktoré vychádzajú z prichádzajúcich udalostí, Network Behavior Anomaly Detection funkcionalitu. |  |  |
|  | Riešenie musí podporovať schopnosť monitorovať históriu útokov (typov udalostí). |  |  |
|  | Riešenie musí podporovať schopnosť korelovať udalosti DHCP, VPN a Active Directory a sledovať priebeh používateľskej relácie v rámci celej organizácie. |  |  |
|  | Riešenie musí obsahovať funkcionalitu behaviorálnej analýzy používateľov. Táto funkcionalita musí využívať algoritmy strojového učenia, musí byť úzko previazaná so zvyškom systému a musí byť spravovaná z jednotného rozhrania správcovskej konzoly SIEM systému. Systém musí obsahovať základné out-of-the-box pravidlá pre funkcionalitu behaviorálnej analýzy používateľov. |  |  |
|  | Riešenie musí ponúkať zobrazenie upozornenia vo webovej konzole riešenia a zasielanie upozornení administrátorom (email, syslog, atď.). |  |  |
|  | Riešenie musí poskytovať možnosť zasielania upozornení na základe detegovanej hrozby, anomálie, porušenia bezpečnostnej politiky alebo prekročenia nastavených limitov. Riešenie musí umožňovať zasielanie upozornení pri výpadku zberu udalostí zo zariadení. |  |  |
|  | Riešenie musí podporovať nastavenie konkrétnej akcie (napr. zaslanie e-mailu, notifikácie alebo spustenie vopred definovaného skriptu), ktorá bude vykonaná v závislosti na spracovanej udalosti alebo výsledku korelačného pravidla. |  |  |
|  | Riešenie musí umožňovať zreťazenie udalostí do jedného záznamu o incidente, takže ak korelačná analýza označí viacero činností, ktoré súvisia s jedným útokom, riešenie vygeneruje iba jeden incident. |  |  |
|  | Riešenie musí v centrálnej webovej konzole umožňovať vykonávanie kombinovaných vyhľadávaní aj v indexovaných audítorských dátach s použitím regulárnych výrazov a fulltextového vyhľadávania v neštruktúrovanom texte súčasne. |  |  |
|  | Riešenie musí byť schopné udržiavať konzistentnú databázu zariadení aj v prípadoch, keď niektoré zariadenia v sieti často menia svoju IP adresu. |  |  |
|  | Riešenie musí poskytovať pokročilé detailné vyhľadávania tzv. Drill-down s možnosťou filtrácie až na úroveň IP adresy, typu udalosti, protokolu, portu atď. |  |  |
|  | Riešenie musí podporovať zrozumiteľný spôsob vyhľadávania s podporou zadaní dotazu s použitím Booleovej logiky alebo pomocou regulárneho výrazu. |  |  |
|  | Riešenie musí obsahovať predpripravené (out-of-box) reporty, ktoré je možné začať používať ihneď po inštalácii. |  |  |
|  | Riešenie musí umožňovať vytvárať vlastné reporty pomocou grafického rozhrania bez nutnosti zostavovať SQL dotazy. |  |  |
|  | Riešenie musí podporovať nezmenenú funkcionalitu reportingu aj pri zmene alebo náhrade niektorých technológií ako napr. firewallu alebo IDS. |  |  |
|  | Riešenie musí umožňovať pre budúce rozšírenie vzdialený zber logov lokálnym kolektorom s následným preposielaním v komprimovanej a šifrovanej podobe v rámci riešenia. |  |  |
|  | Riešenie musí umožňovať vykonávať automatické aktualizácie riešenia bez pomoci profesionálnych služieb výrobcu. |  |  |
|  | Riešenie musí obsahovať mechanizmus na internú kontrolu stavu komponentov riešenia a následného upozornenia administrátora v prípade problému. |  |  |
|  | Riešenie musí natívne podporovať budúce rozšírenie o nasadenie v režime vysokej dostupnosti bez nutnosti využitia ďalších softvérov iných výrobcov alebo riešení tretích strán. |  |  |
|  | Režim vysokej dostupnosti musí byť možné pripojiť v akejkoľvek fáze, bez nutnosti reinštalácie a celého riešenia. |  |  |
|  | Riešenie musí obsahovať mechanizmus pre zabezpečenie integrity ukladaných dát. |  |  |
|  | Riešenie musí obsahovať mechanizmus pre plánované archivovanie uložených dát na externé úložisko. |  |  |
|  | Riešenie musí obsahovať funkcionalitu automatickej tvorby záloh konfigurácie s následnou možnosťou obnovy. |  |  |
|  | Riešenie musí podporovať integráciu pomocou otvoreného API rozhrania. API môže slúžiť pre strojovú interakciu s riešením alebo pre integráciu s riešeniami tretích strán. |  |  |
|  | Riešenie musí umožňovať overenie používateľov pomocou integrácie s adresárovým systémom Active Directory. |  |  |
|  | Riešenie musí umožňovať prácu s reputačnými službami výrobcu alebo s reputačnými službami tretích strán. Reputačné služby poskytujú napríklad IP geolokáciu, botnet kanály atď. Súčasťou riešenia bude aj licencia pre využitie reputačných služieb výrobcu. |  |  |
|  | Riešenie musí umožňovať rozšírenie funkcionality pomocou aplikačného frameworku s verejne dostupným obsahom. |  |  |
|  | Riešenie musí podporovať agregáciu záznamov o sieťovej prevádzke z oboch strán dátového toku do jedného záznamu popisujúceho obojsmernú komunikáciu. |  |  |
|  | Riešenie musí umožňovať dodatočné pridanie integrovaného manažmentu rizík na základe sieťových tokov a konfiguráciu aktívnych prvkov do GUI. |  |  |
|  | Riešenie musí mať schopnosť dodatočne zapojiť umelú inteligenciu do vyšetrovania incidentov v rámci jednotného rozhrania SIEM konzoly. |  |  |
|  | Medzi schopnosti umelej inteligencie musí patriť aspoň doplňovanie informácií o hrozbách nájdených v incidentoch a zobrazovanie informácií o ich možnom šírení na ďalšie prvky v infraštruktúre, vrátane vizualizácie. Umelá inteligencia musí vedieť spojiť dohromady lokálne zozbierané informácie spolu s informáciami zozbieraným externe zo znalostných báz. |  |  |
|  | Umelá inteligencia musí v rámci ponúkaného riešenia sledovať históriu riešenia útokov bezpečnostnými analytikmi a na jej základe odporúčať ďalšie kroky. |  |  |
| Záručné podmienky | Podpora a údržba pre HW zariadenie a softvér musí zahŕňať upgrade a aktuálne opravné balíky (fixies, patch) a musí byť realizovaná onsite v režime 24x7 s reakčnou dobou pri kritických problémoch 2 hodiny a odstránenie vady najbližší pracovný deň. |  |  |
|  | Softvérové licencie riešenia vrátane trojročnej údržby a podpory podľa špecifikácie komponentov riešenia. |  |  |

### Riešenie pre centrálny zber logov

Údaje o ponúkanom zariadení/systéme:

Výrobca: <doplniť>

Model: <doplniť>

Konfigurácia: <doplniť detailnú konfiguráciu ponúkaného zariadenia/systému>

Odkaz na produktovú dokumentáciu na stránkach výrobcu (link): <doplniť link, kde je možné overiť parametre ponúkaných produktov>

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Parameter riešenia pre centrálny zber logov - výkon | Min. 500 Events per Second |  |  |
| Funkčné požiadavky | Riešenie musí licenčne a výkonovo podporovať spracovanie minimálne 500 EPS (Events per second). |  |  |
|  | Riešenie musí byť schopné ukladať interne (tzv. online) aspoň 10 TB dát. |  |  |
|  | Riešenie musí pre zber udalostí podporovať protokoly: minimálne Syslog, Windows Events Collection (WinRE / RPC), FTP, SCP, SNMP, ODBC / JDBC, log file. |  |  |
|  | Riešenie musí podporovať ukladanie prichádzajúcich udalostí v štandardizovanom formáte a zároveň aj v originálnom „raw“ formáte. |  |  |
| Záručné podmienky | Podpora a údržba softvéru musí zahŕňať upgrade a aktuálne opravné balíky (fixies, patch) a musí byť realizovaná onsite v režime 24x7 s reakčnou dobou pri kritických problémoch 2 hodiny a odstránenie vady najbližší pracovný deň |  |  |
|  | Softvérové licencie riešenia vrátane trojročnej údržby a podpory podľa špecifikácie komponentov riešenia. |  |  |

### Softvér zberu udalostí zo systémov tretích strán

Údaje o ponúkanom zariadení/systéme:

Výrobca: <doplniť>

Model: <doplniť>

Konfigurácia: <doplniť detailnú konfiguráciu ponúkaného zariadenia/systému>

Odkaz na produktovú dokumentáciu na stránkach výrobcu (link): <doplniť link, kde je možné overiť parametre ponúkaných produktov>

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Funkčné požiadavky | Riešenie musí podporovať zber udalostí z rôznych prostredí ako sú Windows a Linux prostredia, bezpečnostných a sieťových systémov, databáz a súborov. |  |  |
|  | Riešenie musí umožňovať vzdialený zber logov lokálnym kolektorom s následným preposielaním v komprimovanej a šifrovanej podobe v rámci riešenia pre budúce rozšírenie. |  |  |
|  | V prípade výpadku spojenia musí lokálny kolektor umožňovať dočasné ukladanie zbieraných dáta v rámci riešenia. |  |  |
|  | Riešenie musí podporovať integráciu pomocou otvoreného API rozhrania. API môže slúžiť pre strojovú interakciu s riešením alebo pre integráciu s riešeniami tretích strán. |  |  |
|  | Riešenie musí umožňovať zber udalostí (logov) bez nutnosti inštalovať agenta na cieľový systém. |  |  |
|  | Riešenie musí v prípade potreby umožňovať inštaláciu agenta na cieľový systém na zber udalostí z Microsoft Windows prostredia. |  |  |
| Záručné podmienky | Podpora a údržba pre softvér musí zahŕňať upgrade a aktuálne opravné balíky (fixies, patch) onsite v režime 24x7 s reakčnou dobou pri kritických problémoch 2 hodiny a odstránenie vady najbližší pracovný deň |  |  |
|  | Softvérové licencie riešenia vrátane trojročnej údržby a podpory podľa špecifikácie komponentov riešenia. |  |  |

### Uvedenie SIEM a centrálneho zberu logov do prevádzky

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Požiadavky – rozsah služieb | Vypracovanie dokumentácie návrhu riešenia  Príprava a inštalácia komponentov SIEM  Konfigurácia komponentov  Konfigurácia sieťových nastavení  Integrácia so službami  Pripojenie dátových zdrojov out-of-box - všetkých, ktoré výrobca podporuje  Príprava pripojenia nepodporovaných zdrojov dát - parsovanie užitočných polí, normalizácia, kategorizácia (max. 3)  Implementácia štandardných use-case (out-of-box)  Vytvorenie špecifických use-case (max. 5)  Príprava reportingu, customizovaných dashboardov (max. 10)  Nastavenie zálohovania  Otestovanie funkčnosti podľa navrhnutého testovacieho scenára a optimalizácia  Vypracovanie a dodanie projektovej dokumentácie v rozsahu dokumentácia výrobcu, technická dokumentácia popisujúca skutočné vyhotovenie, používateľská príručka  Školenie používateľov podľa definovaných rolí |  |  |

## Systém na analýzu sieťovej prevádzky

Aktuálne nie je sieťová prevádzka monitorovaná a analyzovaná. Po implementácii systému bude vnútorná komunikácia ako aj komunikácia z a do internetu monitorovaná a vyhodnocovaná s cieľom proaktívnych opatrení aplikovaných v reálnom čase a prepojená na SIEM.

### Zariadenie na monitorovanie sieťovej premávky

Údaje o ponúkanom zariadení/systéme:

Výrobca: <doplniť>

Model: <doplniť>

Konfigurácia: <doplniť detailnú konfiguráciu ponúkaného zariadenia/systému>

Odkaz na produktovú dokumentáciu na stránkach výrobcu (link): <doplniť link, kde je možné overiť parametre ponúkaných produktov>

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Výkonnosť | Min. 1,45 Mp/s na monitorovací port |  |  |
| Porty | Min. 4 porty  Možnosť nastavenia rýchlosti monitorovanej linky - minimálne možnosti - 4x 10/100/1000Mb/s na metalických rozhraniach. |  |  |
| Manažment rozhranie na lokalitu | Min. 1 x (administratívne) porty 10/100/1000 Mb/s pre zabezpečenú vzdialenú správu a prenos Netflow/sFlow/IPFIX dát, dohľad a konfiguráciu - SSH, HTTPS. |  |  |
| Funkčné požiadavky | Časová synchronizácia zariadenia proti centrálnemu zdroju času na sieti. |  |  |
|  | Možnosť integrácie do dohľadového systému pre kontrolu dostupnosti a vyťaženia zdrojov technológiou SNMP. |  |  |
|  | Vzorkovanie na úrovni paketov a na úrovni tokov. |  |  |
|  | Podpora protokolov pre výmenu dát: minimálne Netflow/sFlow/IPFIX. |  |  |
|  | Podpora autentizácie voči LDAP (Active Directory). |  |  |
|  | Možnosť exportovať štatistiky o sieťovej prevádzke (tokov) pomocou spoľahlivého a zabezpečeného komunikačného kanála podľa štandardu RFC 7011. |  |  |
|  | Monitorovanie a reportovanie MAC adries vo flow štatistikách. Možnosť použiť MAC adresu ako položku kľúča flow záznamu. |  |  |
|  | Možnosť deduplikovať pakety priamo na zariadení. |  |  |
|  | Vstavaný Netflow/sFlow/IPFIX kolektor o kapacite min. 1TB. |  |  |
| Prevedenie | HW appliance/zariadenie. |  |  |
|  | Inštalácia do Rack-u |  |  |
| Záručné podmienky | Min. 3 roky |  |  |
|  | Výmena HW 8x5xNBD. |  |  |
|  | Možnosť kontroly kvality (Health check) od výrobcu riešenia po implementácii, konfigurácii a doladení. |  |  |

### Zariadenie na zber a ukladanie sieťovej premávky

Údaje o ponúkanom zariadení/systéme:

Výrobca: <doplniť>

Model: <doplniť>

Konfigurácia: <doplniť detailnú konfiguráciu ponúkaného zariadenia/systému>

Odkaz na produktovú dokumentáciu na stránkach výrobcu (link): <doplniť link, kde je možné overiť parametre ponúkaných produktov>

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Výkonnosť | Spracovanie min. 140 000 fps (dátových tokov za sekundu) |  |  |
| Kapacita úložiska | Min. 5,5 TB (RAID5), min. 64 GB RAM |  |  |
| Funkčné požiadavky | Granularita vizualizácie: spracovanie dátových tokov / paketov a vizualizácia s možnosťou výberu z niekoľkých možností, napr. 5-minútových, 1-minútových alebo 30-sekundových intervalov. |  |  |
|  | Podpora štandardov dátových tokov: min. Netflow, sFlow, IPFIX, jFlow, cflowd, NetStreamsFlow a ich zber z desiatok zdrojov v sieti. |  |  |
|  | Správa používateľov a prístupových práv na zariadeniach prostredníctvom používateľských rolí. Separácia dát s obmedzeným prístupom pre jednotlivé role/používateľov. |  |  |
|  | Možnosť dohľadania ľubovoľnej komunikácie až na úroveň jednotlivých flow záznamov, priebežné grafy prevádzky, top štatistiky, reporty, alerty, databázy aktívnych zariadení na sieti vrátane identifikácie zariadení. |  |  |
|  | Vizualizácia štatistických dát podľa objemu (min . počet prenesených bytov, tokov, paketov), IP prevádzky (min. TCP, UDP, ICMP, ostatné) alebo protokolu (min. HTTP, IMAP, SSH), vrátane plnej konfigurácie grafov a pohľadov používateľom. |  |  |
|  | Riešenie musí poskytovať možnosť jednoduchej konfigurácie pomocou dostupných konfiguračných šablón, ktoré umožňujú výber z dostupných prednastavení a ich aplikáciou vytvárať profily, kapitoly, reporty, widgety a dashboardy bez nutnosti manuálnej konfigurácie. |  |  |
|  | Riešenie poskytuje zabezpečenú vzdialenú správu, dohľad a konfiguráciu – minimálne cez SSH, HTTPS. |  |  |
|  | Podpora autentizácie voči LDAP (Active Directory). |  |  |
|  |  |  |  |
|  | Riešenie musí poskytovať možnosť časovej synchronizácie zariadenia proti centrálnemu zdroju času na sieti. |  |  |
|  | Riešenie umožňuje použitie DNS cache na zariadení pre rýchlejší preklad IP adries na doménové mená. |  |  |
|  | Riešenie poskytuje podporu pre monitorovanie rozšírených L3 / L4 informácií – minimálne TTL (Time to live), TCP Window size, TCP SYN. |  |  |
|  | Riešenie umožňuje monitorovanie a reportovanie MAC adries vo flow štatistikách. Možnosť použiť MAC adresu ako položku kľúča flow záznamu. |  |  |
|  | Riešenie umožňuje spracovanie dátovej prevádzky min. IPv4 a IPv6, VLAN, MPLS, AS, HTTP, HTTPS (SNI), VoIP, DNS, DHCP,SMB / CIFS a emailovej prevádzky. |  |  |
|  | Riešenie obsahuje možnosť analýzy oneskorenia na sieti min. RTT, SRT, delay, jitter, retransmisiu, out-of-order pakety ako súčasť flow štatistík. |  |  |
|  | Riešenie podporuje monitoring aktívnych zariadení na sietí a viditeľnosť do šifrovanej komunikácie SSL/TLS zahŕňajúcu minimálne verziu protokolu, šifrovací algoritmus, cipher suite, detaily certifikátu. |  |  |
|  |  |  |  |
|  | Riešenie podporuje prijímanie a preposielanie IPFIX dát pomocou spoľahlivého TCP spojenia s možnosťou šifrovania (TCP/TLS) podľa štandardu RFC 7011. |  |  |
|  | Riešenie podporuje generovanie štatistík a podrobných výpisov nad voliteľnými časovými intervalmi s voliteľnými filtrami. Rôzne formáty výstupov, minimálne PDF, CSV. |  |  |
|  | Riešenie podporuje monitorovanie zariadení pripojených k dátovej sieti, dlhodobú históriu aktívnych zariadení, identifikáciu na základe IP adresy, MAC adresy, sledovanie VLAN, operačného systému, prihláseného používateľa na danom zariadení. |  |  |
|  | Kolektor musí poskytovať dokumentované API pre získavanie a spracovanie dát. Prostredníctvom API je možné kolektor tiež konfigurovať (napr. definovať vlastné prehľady, reporty, apod.). |  |  |
|  | Kolektor musí poskytovať centralizovaný dashboard s možnosťou tvorby vlastných náhľadov a widgetov, ktorý poskytuje preddefinované náhľady na používané služby na sieti (napr. sociálne siete, videokonferčné aplikácie, antivírusové aplikácie, služby verejných cloudov, Office 365 a pod. pre rýchlejšiu konfiguráciu) a umožňuje tieto dashboardy zdieľať pre jednotlivé používateľské role. |  |  |
| Prevedenie | HW appliance/zariadenie |  |  |
|  | Inštalácia do racku |  |  |
| Záručné podmienky | Min. 3 roky |  |  |
|  | Výmena HW 8x5xNBD. |  |  |
|  | Možnosť kontroly kvality (Health check) od výrobcu riešenia po implementácii, konfigurácii a doladení. |  |  |

### Detekcia anomálií v sieti

Údaje o ponúkanom zariadení/systéme:

Výrobca: <doplniť>

Model: <doplniť>

Konfigurácia: <doplniť detailnú konfiguráciu ponúkaného zariadenia/systému>

Odkaz na produktovú dokumentáciu na stránkach výrobcu (link): <doplniť link, kde je možné overiť parametre ponúkaných produktov>

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Výkonnosť | Min. 4800 fps (dátových tokov / s) / min. 4 rozdielnych dátových zdrojov (aktívny prvok, sieťová sonda, subnet, sieťový segment a pod.) |  |  |
| Forma | Softvér |  |  |
| Architektúra | Architektúra riešenia umožňuje streamové spracovávanie flow dát pre rýchlu detekciu bezpečnostných alebo prevádzkových anomálií. |  |  |
| Funkčné požiadavky | Riešenie musí umožňovať spravovať zdroje sieťových tokov, umožňuje dočasne pozastaviť príjem tokov a indikovať poruchu zdroja sieťových tokov. |  |  |
|  | **Minimálne detekčné mechanizmy**:  Detekcia skenovania portov, slovníkové útoky, útoky odopretia služieb (DoS), útoky na sieťové protokoly SSH, RDP, Telnet.  Detekcia anomálií v DNS, DHCP, SMTP, detekcia multicast prevádzky a neštandardnej komunikácie.  Detekcia P2P sietí a anonymizačných služieb (napr. TOR) a VPN komunikácie.  Detekcia udalostí na základe „Threat Intelligence“ dát (komunikácia s botnet C&C) aktualizovaných najmenej každých 6 hodín.  Detekcia nadmernej záťaže siete, výpadkov služieb, chýbajúcich reverzných DNS záznamov, nových a cudzích zariadení pripojených k sieti.  Detekcia NAT. |  |  |
|  | Riešenie musí byť schopné k jednotlivým detekciám vytvárať a evidovať udalosti a umožňovať ich analýzu v používateľskom prostredí. |  |  |
|  | Detekčné mechanizmy je možné konfigurovať rôznymi spôsobmi (napr. s rôznou citlivosťou) pre štatistiky z rôznych segmentov siete (napr. LAN nebo prestup do internetu, DC a pod.). |  |  |
|  | Riešenie umožňuje detekciu sieťových anomálií na základe predikcie budúceho správania siete s využívaním znalosti histórie komunikácie. |  |  |
|  | Prípadné udalosti, ktoré predstavujú falošné poplachy (false positives) je možné odstrániť prostredníctvom jednoduchej konfigurácie pravidiel vylúčenia falošných poplachov v používateľskom rozhraní. |  |  |
|  | Riešenie umožňuje zastaviť a opäť spustiť pravidlo falošného poplachu, aby bolo možné overiť jeho požadovanú funkčnosť pri bežnej prevádzke. |  |  |
|  | Pre definíciu falošných poplachov je možné využiť filtre, ktoré môžu byť upravované nezávisle na danej definícii pravidla falošného poplachu. |  |  |
|  | Riešenie obsahuje preddefinované priority udalostí s možnosťou používateľského nastavenia závažnosti udalostí na základe IP adresných rozsahov, typov udalostí, miest výskytu alebo detailov udalosti. Jedna udalosť môže mať v závislosti na konfigurácii priradených viac priorít. |  |  |
|  | Udalosti je možné automaticky exportovať vo formáte CEF, protokolom Syslog. |  |  |
|  | Riešenie musí umožňovať integráciu so systémami typu SIEM alebo log management. Súčasťou exportu musí byť event ID, ktoré jednoznačne identifikuje danú udalosť. |  |  |
|  | Udalosti je možné reportovať do dohľadových systémov prostredníctvom funkcionality SNMP trap. |  |  |
|  | Riešenie je schopné s pomocou zabezpečeného komunikačného rozhrania získať ďalšie informácie k IP adrese z adresárových služieb AD/LDAP. |  |  |
|  | Riešenie umožňuje notifikácie o detegovaných udalostiach prostredníctvom e-mailu s možnosťou pripojiť k emailovému reportu vzorku flow dát, na základe ktorých bola udalosť detegovaná. |  |  |
|  | Riešenie umožňuje vizualizáciu priebehu prevádzky s vyznačením detegovaných udalostí v závislosti od nastavenej závažnosti udalostí. |  |  |
|  | Riešenie detekcie anomálií poskytuje dokumentované API pre získavanie a spracovanie udalostí. Prostredníctvom API je možné systém detekcie anomálií takisto konfigurovať (napr. vytvárať filtre, meniť nastavenia detekčných metód a pod.). |  |  |
|  | Riešenie umožňuje definovať vlastné detekčné metódy pomocou poskytnutých príkazov, ktoré vyhľadávajú vo flow štatistikách (vrátane informácií z aplikačnej vrstvy) špecifické vzory správania. Udalosti detegované vlastnými metódami sú spracovávané štandardne ako udalosti z dostupných detekčných metód (notifikácie, reportovanie, atď.). |  |  |
|  | Na výskyt udalosti je možné automaticky reagovať spustením používateľsky definovaných skriptov. |  |  |
|  | Riešenie musí umožňovať analýzu šifrovanej komunikácie pre potreby detekcie bezpečnostných hrozieb v šifrovane prevádzke a podporu manažmentu politík používaných šifrovacích mechanizmov. |  |  |
|  | Riešenie musí mať vstavaný IDS (Intrusion Detection System). |  |  |
|  | Riešenie musí mapovať a vizualizovať MITTRE ATT&CK taktiky a techniky voči jednotlivým udalostiam pre výskyt anomálií a bezpečnostných hrozieb na sieti. |  |  |
|  | Riešenie musí umožňovať on-demand, plánovaný a automatizovaný záchyt dátovej prevádzky L2-L7 v prípade identifikácie škodlivej udalosti, útoku, kybernetického bezpečnostného incidentu a tento záchyt je možné uložiť vo forme PCAP pre forenzné činnosti. Riešenie umožňuje analyzovať sieťovú prevádzku a výsledky analýzy prezentuje v zrozumiteľnej podobe v rámci udalostí, ktoré popisujú, ako jednotlivé komunikácie v zázname prevádzky prebiehali. Udalosti sú rozdeľované podľa závažnosti do niekoľkých úrovní a indikujú problémy vzniknuté v sieťovej prevádzke na podporovaných protokoloch. Pre jednotlivé udalosti je možné zobraziť detail, ktorý obsahuje informácie o komunikujúcich stranách, použitých portoch, čase a ďalšie informácie z paketov a použitých protokolov. V prípade udalostí popisujúcich neštandardné stavy či chyby systém zobrazuje detailný popis vzniknutej situácie pomocou chybových hlášok. |  |  |
| Záručné podmienky | Min. 3 roky |  |  |
|  | Výmena HW 8x5xNBD. |  |  |
|  | Možnosť kontroly kvality (Health check) od výrobcu riešenia po implementácii, konfigurácii a doladení. |  |  |

### Záznamové zariadenie sieťovej premávky

Údaje o ponúkanom zariadení/systéme:

Výrobca: <doplniť>

Model: <doplniť>

Konfigurácia: <doplniť detailnú konfiguráciu ponúkaného zariadenia/systému>

Odkaz na produktovú dokumentáciu na stránkach výrobcu (link): <doplniť link, kde je možné overiť parametre ponúkaných produktov>

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
|  |  |  |  |
| Forma | Softvér |  |  |
| Funkčné požiadavky | Full packet capture vo formáte PCAP. |  |  |
|  | Umožňuje filtrovanie dátových tokov na základe rôznych kritérií, minimálne IP adresa, CIDR, MAC adresa, protokol, port, VLAN tag, MPLS label. |  |  |
|  | Rolling capture buffer – ukladá prvých N paketov dátového toku. |  |  |
|  | PCAP analýza a diagnostika s podporou protokolov minimálne: DNS, DHCP, FTP, IMAP, IMF, POP, SIP, SLAAC, SMB, SMTP, IP, TCP, SSL, HTTP. |  |  |
|  | Automatizované zaznamenávanie pomocou nástroja na detekciu anomálií. |  |  |
|  | REST API na prístup k PCAP súborom |  |  |
| Záručné podmienky | Min. 3 roky |  |  |
|  | Výmena HW 8x5xNBD. |  |  |
|  | Možnosť kontroly kvality (Health check) od výrobcu riešenia po implementácii, konfigurácii a doladení. |  |  |

### Nasadenie a uvedenie systému na analýzu sieťovej prevádzky do prevádzky

Nasadenie a uvedenie uceleného riešenia monitorovania a súvisiacich komponentov (kolektovanie, ochrana DDoS, detekcia anomálií a záznamu) do prevádzky.

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Požiadavky na nasadenie a uvedenie do prevádzky | Vypracovanie návrhu riešenia  Príprava a inštalácia komponentov  Konfigurácia komponentov  Integrácia so službami – AD, SIEM  Pripojenie dátových zdrojov  Nastavenie zálohovania  Otestovania a ladenie  Školenie |  |  |
| Vytvorenie dokumentácie riešenia | Dokumentácia skutočného vyhotovenia  Používateľská príručka |  |  |

## Systém pre ochranu dokumentov

Aktuálne nie je implementovaná žiadna ochrana na úrovni dokumentov. Požadovaný systém bude postavený na súlade dvoch princípov: ochrana samotných dokumentov a ochrana pred ich neoprávnenou distribúciou alebo použitím.

Systém pre ochranu dokumentov musí priamo v dokumente umožniť riadenie prístupu jednotlivých používateľov (interných alebo externých) k danému dokumentu. Okrem priameho zneprístupnenia dokumentu systém umožní aj povolenie iba vybraných operácií s dokumentom.

### Softvér pre ochranu dokumentov

Údaje o ponúkanom zariadení/systéme:

Výrobca: <doplniť>

Model: <doplniť>

Konfigurácia: <doplniť detailnú konfiguráciu ponúkaného zariadenia/systému>

Odkaz na produktovú dokumentáciu na stránkach výrobcu (link): <doplniť link, kde je možné overiť parametre ponúkaných produktov>

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Klasifikácia súborov | Vytváranie vlastných klasifikácií  Manuálna a automatická klasifikácia súborov  Označovanie klasifikácie v dokumentoch  Zmena klasifikácie  Odstránenie klasifikácie  Automatická klasifikácia súborov na file serveroch  Automatická klasifikácia e-mailových správ  Podpora predovšetkým základných typov súborov MS Office, vrátane e-mailových správ, PDF súborov a obrázkov  Integrácia so správcami súborov  Integrácia s aplikáciami Office |  |  |
| Šifrovanie súborov | Dĺžka kľúča pre šifrovanie súborov min. 128 bitov  Dĺžka kľúča pre šifrovanie kľúčov pre šifrovanie súborov min. 2048 bitov  Podpisovanie certifikátov min. SHA-256  Možnosť použitia vlastného kľúča pre šifrovanie kľúčov pre šifrovanie súborov |  |  |
| Prístup k súborom | Prístup k súborom na základe klasifikácie  Manuálne definovanie používateľov s oprávneniami  Rôzne možnosti úrovne prístupu  Zmena oprávnení  Zrušenie oprávnení  Možnosť prístupu interných aj externých používateľov  Monitorovanie prístupov k dokumentom, zasielanie e-mailových oznámení o prístupe  Automatické prideľovanie prístupov na file serveroch  Možnosť získania prístupu k súborom v prípade nemožnosti prístupu vlastníka  Podpora predovšetkým základných typov súborov MS Office, PDF súborov, textových súborov a obrázkov  Integrácia so správcami súborov a s aplikáciami Office |  |  |
| Licencia | Licencia pre dodávaný systém min. na 3 roky. |  |  |

### Vypracovanie návrhu riešenia systému pre ochranu dokumentov

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Vypracovanie návrhu riešenia | Popis funkcionality, ktorá sa bude používať  Používané služby a komponenty  Návrh architektúry riešenia  Návrh topológie riešenia  Požiadavky na licencie  Hardvérové požiadavky  Softvérové požiadavky  Požiadavky na komunikáciu  Požiadavky na infraštruktúrne služby (Active Directory, group policy a ďalšie)  Popis konfigurácie jednotlivých funkcií, služieb a komponentov  Zálohovanie a obnova systému, konfigurácie a dát |  |  |

### Konfigurácia systému pre ochranu dokumentov

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Konfigurácia softvéru | Služby a komponenty pre používanú funkcionalitu  Vytvorenie klasifikácií podľa požiadaviek  Automatická klasifikácia súborov na file serveri  Automatická klasifikácia e-mailových správ  Konfigurácia oprávnení podľa požiadaviek  Konfigurácia oznámení  Integrácia so správcami súborov a aplikáciami Office |  |  |

### Overovanie a ladenie systému pre ochranu dokumentov

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Overovanie a ladenie | Manuálna a automatická klasifikácia jednotlivých typov súborov  Automatická klasifikácia súborov na file serveroch  Automatická klasifikácia e-mailových správ  Definovanie oprávnení pre rôzne úrovne prístupu  Prístup oprávnených používateľov pre jednotlivé úrovne prístupu  Prístup interných a externých používateľov  Monitorovanie prístupov k dokumentom, zasielanie e-mailových oznámení o prístupe  Automatické prideľovanie prístupov na file serveroch  Získanie prístupu k súborom v prípade nemožnosti prístupu vlastníka  Integrácia so správcami súborov a aplikáciami Office |  |  |

### Vypracovanie dokumentácie riešenia systému pre ochranu dokumentov

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Vypracovanie dokumentácie riešenia | Popis funkcionality, ktorá sa používa  Používané služby a komponenty  Popis architektúry riešenia a obrazová schéma  Popis topológie riešenia a obrazová schéma  Používané licencie  Popis hardvérovej konfigurácie  Zoznam nainštalovaného softvéru  Popis komunikácie  Popis používaných infraštruktúrnych služieb (Active Directory, group policy a ďalšie)  Popis konfigurácie jednotlivých funkcií, služieb a komponentov  Popis zálohovania a obnovy systému, konfigurácie a dát |  |  |
| Vypracovanie používateľskej príručky | Klasifikácia dokumentov (automatická a manuálna)  Zmena klasifikácie  Zrušenie klasifikácie  Používanie klasifikovaných dokumentov  Definovanie oprávnení (manuálne a na základe klasifikácie)  Zmena oprávnení  Zrušenie oprávnení  Používanie dokumentov s definovanými oprávneniami  Sledovanie prístupu k súborom  Získanie prístupu k súborom v prípade nemožnosti prístupu vlastníka |  |  |

### Zaškolenie administrátorov systému pre ochranu dokumentov

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Zaškolenie administrátorov | Konfigurácia systému a komponentov  Vytvorenie klasifikácií  Manuálna a automatická klasifikácia dokumentov  Konfigurácia automatickej klasifikácie súborov na file serveri  Konfigurácia automatickej klasifikácie e-mailových správ  Konfigurácia oprávnení  Konfigurácia oznámení  Konfigurácia automatického prideľovania prístupov na file serveroch  Získanie prístupu k súborom v prípade nemožnosti prístupu vlastníka  Integrácia so správcami súborov a aplikáciami Office  Konfigurácia zálohovania  Postup pre obnovu systému |  |  |

## Systém pre riadenie identít a autentifikačných prostriedkov - dvojfaktorová autentifikácia

Aktuálne je aplikovaná centrálna autentifikácia len na báze mena a hesla. Prihlasovanie je cez kontá v Active Directory, avšak len pre časť koncových staníc. Dvojfaktorová autentifikácia (2FA) bude aplikovaná na prihlasovanie sa do vybraných systémov a aplikácií.

### Softvér pre dvojfaktorovú autentifikáciu

Údaje o ponúkanom zariadení/systéme:

Výrobca: <doplniť>

Model: <doplniť>

Konfigurácia: <doplniť detailnú konfiguráciu ponúkaného zariadenia/systému>

Odkaz na produktovú dokumentáciu na stránkach výrobcu (link): <doplniť link, kde je možné overiť parametre ponúkaných produktov>

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Všeobecné požiadavky | Riešenie pre 2-faktorovú autentifikáciu (2FA) určené na generovanie jednorazových hesiel (OTP) pomocou mobilnej aplikácie bežiacej na smartfóne koncového používateľa pristupujúceho k nižšie uvedeným podporovaným službám/aplikáciám.  Jednorazové heslo je potrebné zo strany užívateľa zadať pri prihlasovaní sa do daných služieb/aplikácií spolu so štandardne vyžadovaným používateľským menom a heslom.  Alternatívne musí byť možné v rámci ponúkaného riešenia použiť smerom na mobilné zariadenie koncového používateľa „push notifikáciu“, ktorej schválenie používateľom zabezpečí 2-faktorové overenie jeho prihlásenia.  Alternatívne musí byť možné v rámci ponúkaného riešenia doručenie informácie, potrebnej pre prihlásenie, aj vo forme SMS. Dodávka musí obsahovať aspoň 500 SMS mesačne po dobu 3 rokov. |  |  |
| Počet používateľov | 175 |  |  |
| Systémové požiadavky | Autentifikačný server musí byť podporovaný na niektorom z nasledujúcich serverových operačných systémov : Windows Server 2012 Essentials / 2012 R2 Essentials / Windows Server 2016 /2016 Essentials / 2019 / 2019 Essentials.  Softvér musí podporovať integráciu s webovým rozhraním Outlook Web Access pre Microsoft Exchange 2010/2013/2016/2019.  Softvér musí podporovať integráciu s Microsoft Sharepoint 2010/2013/2016/2019.  Softvér musí podporovať integráciu s programom Microsoft Remote Desktop Web Access.  Softvér musí podporovať integráciu s Microsoft Terminal Services Web Access.  Softvér musí podporovať integráciu s Microsoft Remote Web Access.  Softvér musí podporovať integráciu s RADIUS serverom, ktorý umožňuje autentifikáciu používateľa pre riešenia VPN, ktoré podporujú technológiu RADIUS.  Softvér musí podporovať integráciu s HCL Notes |  |  |
| Požiadavky na mobilnú aplikáciu pre koncového užívateľa | Mobilná aplikácia musí podporovať telefóny s nasledujúcimi operačnými systémami: Android verzia 6 a novší, iOS 9 a novší.  Mobilnú aplikáciu na generovanie OTP (jednorazových hesiel) musí poskytnúť dodávateľ riešenia ako súčasť zakúpenej licencie, čiže v cene riešenia.  Používateľ musí byť schopný dodatočne zabezpečiť mobilnú aplikáciu pomocou PIN kódu.  Mobilná aplikácia nemôže od používateľa vyžadovať aktívne pripojenie na internet, čiže generovanie OTP (jednorazového hesla) musí byť možné offline.  2-faktorová autentifikácia musí byť možná aj pomocou jednorazových hesiel zasielaných používateľovi prostredníctvom SMS.  Aplikácia nainštalovaná na mobilných zariadeniach musí umožňovať generovanie OTP pre viac ako jeden autentifikačný server. |  |  |
| Monitorovanie | Monitorovanie systému a jeho jednotlivých komponentov.  Konfigurácia alertov pre kritické udalosti.  Zasielanie e-mailových notifikácií. |  |  |
| Zabezpečenie | Prístup na základe rolí a skupín objektov.  Vytváranie vlastných rolí s definovanými oprávneniami. |  |  |
| Zálohovanie a obnova | Zálohovanie systému, konfigurácie a dát pre prípad požiadavky na obnovu. |  |  |
| Licencia | Licencia pre dodávaný systém min. na 3 roky. |  |  |

### Vypracovanie návrhu riešenia systému pre dvojfaktorovú autentifikáciu

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Vypracovanie návrhu riešenia | Popis funkcionality, ktorá sa bude používať  Používané služby a komponenty  Návrh architektúry riešenia  Návrh topológie riešenia  Požiadavky na licencie  Hardvérové požiadavky  Softvérové požiadavky  Požiadavky na komunikáciu  Požiadavky na infraštruktúrne služby (Active Directory, group policy a ďalšie)  Konfigurácia jednotlivých funkcií, služieb a komponentov  Zálohovanie a obnova systému, konfigurácie a dát  Certifikačná autorita, čiže systém s certifikačnými autoritami pre vydávanie a manažovanie digitálnych certifikátov podľa štandardu X.509 s nasledovnými vlastnosťami:   * Integrácia do MS Active Directory (AD), možnosť väzby na objekty používateľov a počítačov, autentifikácia s využitím AD * Možnosť vystavenia certifikátov použiteľných pre vzdialený prístup technológiou MS RDP (Remote Desktop Protocol) * Možnosť vystavenia certifikátov použiteľných pre riadenie prístupu do počítačovej siete protokolom 802.1X * Hierarchia certifikačných autorít (CA): offline koreňová CA a online CA pre vydávanie certifikátov * Možnosť nastavenia vlastností certifikátov s použitím šablón * Riešenie pre publikovanie zoznamu zneplatnených certifikátov |  |  |

### Konfigurácia softvéru pre dvojfaktorovú autentifikáciu

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Konfigurácia softvéru | Inštalácia a konfigurácia komponentov.  Konfigurácia užívateľských kont a skupín.  Konfigurácia reportovania.  Konfigurácia zálohovania.  Konfigurácia Certifikačnej autority v zmysle návrhu riešenia |  |  |

### Overovanie a ladenie systému pre dvojfaktorovú autentifikáciu

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Overovanie a ladenie | Prihlasovanie používateľov.  Monitorovanie.  Reportovanie.  Zálohovanie systému a obnova. |  |  |

### Vypracovanie dokumentácie riešenia systému pre dvojfaktorovú autentifikáciu

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Vypracovanie dokumentácie riešenia | Popis funkcionality, ktorá sa používa  Používané služby a komponenty  Popis architektúry riešenia a obrazová schéma  Popis topológie riešenia a obrazová schéma  Používané licencie  Popis hardvérovej konfigurácie  Zoznam nainštalovaného softvéru  Popis komunikácie  Popis používaných infraštruktúrnych služieb (Active Directory, group policy a ďalšie)  Popis konfigurácie jednotlivých funkcií, služieb a komponentov  Popis zálohovania a obnovy systému, konfigurácie a dát  Získanie prístupu v prípade straty zariadenia užívateľa.  Certifikačná autorita.  Vypracovanie používateľskej príručky |  |  |

### Zaškolenie administrátorov systému pre dvojfaktorovú autentifikáciu

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Zaškolenie administrátorov | Konfigurácia systému a komponentov.  Monitorovanie systému a komponentov.  Reporty.  Vytváranie vlastných prehľadov.  Aktualizácia systému.  Riešenie problémov.  Konfigurácia zálohovania.  Postup pre obnovu systému. |  |  |

## Systém pre riadenie prístupov zo vzdialených sietí

Aktuálne sú prostriedky pre vytváranie privátnych sietí VPN využívané len málo a to aj z dôvodu nemožnosti zabezpečiť monitoring aktivity vzdialených používateľov. Požadovaný systém pre riadenie vzdialených prístupov bude podporovať manažment prístupov s previazaním na systém riadenia identít a aj úplné monitorovanie činností vybraných používateľov z externých organizácií, ktorí budú pristupovať k systémom ÚJD (napr. správcovia z dodávateľských organizácií).

### Operačný systém servera pre riadenie prístupov zo vzdialených sietí

Údaje o ponúkanom zariadení/systéme:

Výrobca: <doplniť>

Model: <doplniť>

Konfigurácia: <doplniť detailnú konfiguráciu ponúkaného zariadenia/systému>

Odkaz na produktovú dokumentáciu na stránkach výrobcu (link): <doplniť link, kde je možné overiť parametre ponúkaných produktov>

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Typ licencie | MS WINDOWS Server 2019 STD (min. počet jadier na licenčné pokrytie Servera pre prevádzku softvéru pre riadenie prístupov zo vzdialených sietí) |  |  |
| Množstvo | 1 |  |  |
| SA | Bez SA |  |  |

### Licencie pre pripojenie ku vzdialenej ploche servera pre riadenie prístupov zo vzdialených sietí

Údaje o ponúkanom zariadení/systéme:

Výrobca: <doplniť>

Model: <doplniť>

Konfigurácia: <doplniť detailnú konfiguráciu ponúkaného zariadenia/systému>

Odkaz na produktovú dokumentáciu na stránkach výrobcu (link): <doplniť link, kde je možné overiť parametre ponúkaných produktov>

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Typ licencie | MS Windows server 2019 Remote desktop user CAL |  |  |
| Množstvo | Pre 25 používateľov |  |  |
| SA | Bez SA |  |  |

### Softvér pre server pre riadenie prístupov zo vzdialených sietí

Údaje o ponúkanom zariadení/systéme:

Výrobca: <doplniť>

Model: <doplniť>

Konfigurácia: <doplniť detailnú konfiguráciu ponúkaného zariadenia/systému>

Odkaz na produktovú dokumentáciu na stránkach výrobcu (link): <doplniť link, kde je možné overiť parametre ponúkaných produktov>

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Manažment prístupov | Riešenie musí zabezpečovať bezpečný, riadený a kontrolovaný prístup zo vzdialených sietí pre interných ako aj externých pracovníkov. |  |  |
| Funkčné požiadavky | Riešenie musí poskytovať nástroje na riadenie prístupov zo vzdialených sietí a monitoring činností používateľov pristupujúcich na interné systémy zo vzdialených sietí. |  |  |
|  | Riešenie by malo umožňovať aj správu privilegovaných účtov, riadenie prístupu k týmto účtom a monitoring všetkých aktivít riadených účtov. Používateľské prístupy sa musia riadiť bezpečnostnou politikou, tzn. používateľ má právo prístupu a vidí iba definované účty a systémy. |  |  |
|  | Riešenie musí byť spravované pomocou jednotnej centrálnej správy - prístup k používateľskému rozhraniu je požadovaný cez webový portál s možnosťou overenia pomocou LDAP/MS Active Directory a druhým faktorom (integrácia s riešením, dodávaným v rámci systému pre riadenie identít a autentifikačných prostriedkov - dvojfaktorová autentifikácia).  Riešenie musí umožňovať konfiguráciu systémov pomocou RestAPI - správa používateľov, vytváranie a editácia účtov, zmeny prihlasovacích údajov, ukončenie spojení, nastavenie oprávnení, zmeny politík, systém health monitoring, schvaľovanie požiadaviek, autentizácia, atď. |  |  |
|  | Riešenie musí umožňovať oddelenie prístupových oprávnení a podporovať multitenant prostredie. Používatelia, resp. skupiny používateľov majú prístup len k vybraným účtom, systémom, auditným záznamom, konfiguráciám, atď. Musí umožňovať prideľovanie a riadenie práv na základe rolí. Správca riešenia má povolený prístup iba k vybraným zložkám a vybraným konfiguráciám. |  |  |
|  | Riešenie musí poskytovať vysokú bezpečnosť prenesených a uložených informácii (confidentiality, integrity, availability). Uložené informácie, vrátane záznamov (nahrávok) a spravovaných prihlasovacích údajov, sú uložené v jednej centrálnej a vysoko zabezpečenej databáze. Riešenie musí umožňovať obmedzenie práv správcu systému tak, aby nemal prístup k uloženým prihlasovacím údajom, logom, alebo nahrávkam bez autorizácie vlastníkom dát. Systém ako celok musí byť certifikovaný bezpečnostným štandardom Common Criteria alebo ekvivalentom. |  |  |
|  | Riešenie musí umožňovať integráciu s ticketingovými nástrojmi tretích strán - žiadosť o schválenie prístupu, prístup na základe existujúceho tiketu, atď. |  |  |
|  | Riešenie musí umožňovať plnú integráciu s Microsoft Active Directory na úrovni informácií o používateľoch, príslušnosti k skupinám a emailoch. Integrácia musí umožňovať mapovanie rolí v riešení v nadväznosti na skupiny v AD. |  |  |
|  | Riešenie musí umožňovať vynucovanie silnej autentizácie používateľov na bezpečné vzdialené pripojenie, taktiež na prístup k uloženým údajom. Silnou autentizáciou je myslená minimálna možnosť kombinácie meno/heslo + druhý faktor. Riešenie musí umožňovať integráciu s 2FA nástrojmi tretích strán. |  |  |
|  | Riešenie musí spĺňať štandard FIPS 140-2 a šifrovacie algoritmy minimálne na úrovni AES-256 a RSA-2048. Riešenie umožňuje naplnenie súladu/compliance s požiadavkami legislatívy (ZKB, GDPR, ...), ako aj so štandardmi ako napr. SOX, HIPAA, atď. |  |  |
|  | Riešenie musí umožniť izoláciu vzdialených prístupov na cieľový systém zo vzdialených sietí. Prístup na cieľový systém bude realizovaný cez tzv. terminal/jump server prostredníctvom vybraného komunikačného protokolu, aplikácie a príslušného účtu tak, aby koncový používateľ mohol mať aj obmedzený prístup k prihlasovacím údajom. Izolácia vzdialených prístupov bude možná až na úroveň aplikácie (typu webový prehliadač s konkrétnou URL, MMC konzola s vybraným snap-in, konkrétna aplikácia... napr. MS SQL Management Studio, WinSCP, atď. ). Používateľ nebude mať možnosť pristupovať k iným službám, aplikáciám v rámci daného vzdialeného pripojenia. Po ukončení aplikácie bude vzdialené pripojenie ukončené. Vzdialené pripojenie bude možné nadviazať cez vlastné GUI riešenia, ako aj pomocou štandardných protokolov RDP a SSH a štandardných klientov typu putty a remote desktop manager. |  |  |
|  | Riešenie musí umožniť vzdialený prístup prostredníctvom SSH protokolu pomocou SSH Proxy, kde bude používateľ overený svojimi prihlasovacími údajmi (možnosť párovania s MS Active Directory) a bude pripojený vybraným účtom na cieľový systém bez nutnosti zadávania hesla a v súlade s bezpečnostnými politikami. Pre vzdialený prístup pomocou SSH Proxy je vyžadovaná podpora silnej autentizácie (minimálne integrácia s LDAP, RADIUS, či autentizácie pomocou SSH kľúča). |  |  |
|  | Riešenie musí umožniť pripojenie pomocou webového prehliadača a protokolu HTTPS (nie je nutné otvárať z klientskej stanice RDP/SSH/iné protokoly); medzi používateľom a jump serverom bude vždy otvorený len bezpečný WebSocket protokol (port 443). |  |  |
|  | Riešenie musí umožňovať monitoring a nahrávanie celej relácie a aktivít používateľov vo video formáte s možnosťou kontextového vyhľadávania, bez nutnosti inštalácie agentov na koncový systém. Záznam relácie musí byť vytvorený kontinuálne. V nahrávkach bude možné spätne vyhľadávať pomocou metadát - minimálne pri RDP spustenie aplikácie a udalosti, pri SSH relácii jednotlivé príkazy, pri Webových aplikáciách click na jednotlivé odkazy, pri iných typoch relácii minimálne stlačenia jednotlivých klávesov. Na prehrávanie nahrávok nie je nutné inštalovať nástroje tretích strán (flash, java, codec, atp...) a je dostupné z GUI dodávaného riešenia. |  |  |
|  | Riešenie poskytuje možnosť automaticky vyhodnocovať a označovať nahrávky relácií na základe vybraných spustených príkazov a aplikácií tak, aby bolo možné vyhľadávať potenciálne nebezpečné činnosti. Systém zároveň umožňuje alerting takých udalostí, vrátane možnosti exportu logov v reálnom čase pomocou syslog na SIEM atď. |  |  |
|  | Riešenie obsahuje možnosť automatického pozastavenia, alebo ukončenia potenciálne nebezpečných relácií. Pravidlá na detekciu potenciálne nebezpečných relácií je možné komplexne editovať - typ udalosti, používatelia (možnosť nastavenia výnimky na úrovni skupín v AD) a typ reakcie. |  |  |
|  | Riešenie umožňuje sledovať aktívne relácie ďalším používateľom (napríklad audítor) a v prípade nutnosti ukončiť sledovanú reláciu. Sledovanie „živých“ relácii je tiež možné pomocou webového prehliadača a protokolu HTTPS (nie je nutné otvárať RDP protokol z klientskej stanice). |  |  |
|  | Riešenie umožňuje autorizovanému personálu centrálne vyhľadávať v nahrávkach podľa dátumu, používateľa a spusteného príkazu. Riešenie umožňuje označovať nahrávky relácií pomocou skóre na základe spustených aplikácií, akcií a príkazov v danej relácii. |  |  |
|  | Ako súčasť riešenia je preferovaný aj nástroj umožňujúci vykonávanie analýzy využívania privilegovaných účtov a následnú detekciu potenciálne škodlivého správania , detekciu podozrivých aktivít používateľov v reálnom čase a umožňuje automatické vynucovanie nápravných opatrení - alerting, zmena prihlasovacích údajov, ukončenie/pozastavenie relácií. |  |  |
|  | Riešenie umožňuje vytváranie nových používateľov do systému. Správca riešenia dokáže cez webové rozhranie vytvoriť používateľa, priradiť mu oprávnenia aj s definovaním časového obdobia. Riešenie následne zašle email novému používateľovi a umožní mu bezpečné vzdialené pripojenie. |  |  |
|  | Spojenie medzi externým používateľom a riešením musí byť plne šifrované. Nie je umožnené priame spojenie medzi stanicou používateľa a cieľovým systémom - je využitý princíp bezpečného „jump“ servera. |  |  |
|  | Výrobca riešenia musí poskytovať verejne dostupný (napr. URL na verejnú webovú stránku) zoznam integrovaných riešení na úrovni Remote Session Management, SIEM, atď. |  |  |
|  | Riešenie musí umožňovať integráciu s nástrojmi SIEM - prenos logovaných auditných záznamov, ideálne v reálnom čase pomocou Syslog. |  |  |
|  | Riešenie musí umožňovať integráciu s nástrojmi HSM - uloženie šifrovacích kľúčov k databáze riešenia. |  |  |
| Architektúra | Riešenie musí podporovať nasadenie vo vysokej dostupnosti a vlastné technologické možnosti (bez použitia nástrojov/SW tretích strán) na zabezpečenie High Availability, Disaster Recovery a zálohovania tak, aby boli citlivé dáta stále vysoko zabezpečené a dostupné iba vlastníkom dát. |  |  |
|  | Disaster recovery a HA proces je plne automatický a nie je závislý na nástrojoch tretích strán (napr. MS cluster atď.). |  |  |
|  | Všetky komponenty riešenia musia plniť nároky na vysoké zabezpečenie a automaticky vynucovať tzv. hardening. |  |  |
|  | Riešenie musí umožňovať bezpečné zálohovanie dát systému - zálohy musia byť šifrované a prístup k zálohovaným dátam je umožnený len prostredníctvom zabezpečených Disaster Recovery kľúčov. |  |  |
| Reporting | Riešenie musí umožňovať audit jednotlivých akcií používateľov s privilegovanými účtami - zobrazenie hesla, zmena uložených údajov, vytvorenie relácie. |  |  |
|  | Riešenie musí umožňovať generovanie reportu všetkých aktivít správcu riešenia. |  |  |
|  | Riešenie umožňuje nastavenie prístupu k reportom iba pre vybraných používateľov. |  |  |
|  | Riešenie zaručuje nespochybniteľnú auditovateľnosť jednotlivých operácií, možnosti reportovania a textové logy. |  |  |
|  | Riešenie musí umožňovať nezmazateľnosť logov po dobu minimálne 30 dní. Auditné záznamy musia byť bezpečne uložené v zašifrovanej podobe tak, aby k nim mal prístup iba oprávnený používateľ. |  |  |
| Licenčný model | Riešenie musí byť dimenzované minimálne pre 25 používateľov s plným používateľským prístupom (dostupné všetky funkcie riešenia). Licencia musí byť dimenzovaná na pokrytie minimálne 100 cieľových systémov. Súčasťou licencie musí byť aj pokrytie prípadného budúceho riešenia redundancie všetkých komponentov a taktiež geo-redundancie (aspoň active-passive) s dodatočnou miestnou redundanciou v druhej geolokácii. |  |  |
|  | Licencia zároveň pokrýva možnosť inštalácie testovacieho prostredia s plnou funkcionalitou a v plnom rozsahu. |  |  |
| Záručné podmienky | Dodávka musí obsahovať podporu výrobcu na obdobie min. 3 rokov. Technická podpora musí byť minimálne v rozsahu 8x5.  Softvérové licencie riešenia vrátane trojročnej údržby a podpory podľa špecifikácie komponentov riešenia. |  |  |

### Softvér pre servery, ku ktorým je požadovaný riadený prístup zo vzdialených sietí

Údaje o ponúkanom zariadení/systéme:

Výrobca: <doplniť>

Model: <doplniť>

Konfigurácia: <doplniť detailnú konfiguráciu ponúkaného zariadenia/systému>

Odkaz na produktovú dokumentáciu na stránkach výrobcu (link): <doplniť link, kde je možné overiť parametre ponúkaných produktov>

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Architektúra riešenia | Riešenie musí umožňovať najmä bezagentskú integráciu cieľových systémov. Riešenie musí podporovať bezpečný prístup používateľom cez webový prehliadač bez nutnosti inštalácie VPN. |  |  |
| Podpora bezpečných prístupov pre cieľové systémy | Riešenie musí podporovať minimálne nasledovné cieľové systémy  Windows 7, 8, 8.1, 10 a vyšší, Windows Server 2012, 2016, 2019 ,2022 a vyšší  Active Directory  Windows Services, Windows Scheduled Tasks, IIS Application Pool, Windows Registry COM+  HP iLO, Dell DRAC, IBM  VMware, HyperV, Citrix  Red Hat, Suse  MS SQL, MySQL, PostreSQL, Oracle  Checkpoint, Fortinet, Cisco  Office 365 |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Záručné podmienky | Dodávka musí obsahovať podporu výrobcu na obdobie min. 3 rokov. Technická podpora musí byť minimálne v rozsahu 8x5.  Softvérové licencie riešenia vrátane trojročnej údržby a podpory podľa špecifikácie komponentov riešenia. | Splnenie požiadaviek [áno/nie] | Hodnota parametra |

### Server pre prevádzku softvéru pre riadenie prístupov zo vzdialených sietí

Údaje o ponúkanom zariadení/systéme:

Výrobca: <doplniť>

Model: <doplniť>

Konfigurácia: <doplniť detailnú konfiguráciu ponúkaného zariadenia/systému>

Odkaz na produktovú dokumentáciu na stránkach výrobcu (link): <doplniť link, kde je možné overiť parametre ponúkaných produktov>

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Prevedenie | Optimalizovaný pre umiestnenie do 19" dátového rozvádzača (racku), výška max. 1U  Uchytenie servera v racku na výsuvných koľajniciach |  |  |
| Požiadavky na procesor(y) | Osadený minimálne jeden procesor s parametrami: min. 10 jadier.  Server musí podporovať AVX 512-bit.  Server musí byť preukázateľne schopný dosiahnuť výsledok v teste SPECrate®2017\_int\_base aspoň 50 bodov.  Údaj o výkone musí byť preukázateľný pre konkrétny ponúkaný server na verejne dostupnej stránke https://www.spec.org |  |  |
| Systémová pamäť | Server disponuje min. 16 využiteľnými pamäťovými slotmi, pamäť celkovo rozšíriteľná do min. 2TB  Osadená kapacita: min. 128GB DDR4 3200MHz Registered DIMM, s funkciou detekcie a opravy multibitových chýb, zrkadlenia pamätí, on-line spare pamäte |  |  |
| Subsystém pevných diskov | Server musí podporovať budúce rozšírenie interných pozícií pre 2,5" disky typu hot-swap do počtu min. 10 ks bez potreby pripojenia externej diskovej police.  Osadené min. 960GB NVME PCIe 3.0 x4 typu hot swap, nakonfigurované v RAID 1.  Min. prepisová kapacita 1366TB alebo min 0,8 DWPD. Minimálne výkonnostné parametre disku: 400tis IOPS pri čítaní (4kB bloky) a 36tis pri zápise (4kB bloky). |  |  |
| NVMe | Podpora NVMe diskov |  |  |
| Sieťové adaptéry | Min. 1x 2-portový 1Gbps ethernet adaptér pre pripojenie k externému prostrediu metalickým rozhraním typu RJ45  Dedikovaný port pre manažment servera |  |  |
| Dátové a video konektory | Min. 1x USB na prednom paneli  Min. 1x USB na pripojenie mobilného zariadenia typu smartfón alebo tablet pre použite manažovacej aplikácie za účelom fyzického servisovania zariadenia  Min. 2x USB porty a 1x VGA port na zadnom paneli |  |  |
| Rozširujúce sloty | Min. 2x PCIe x16  min. 1x dedikovaný PCI slot pre HW Raid adapter |  |  |
| Bezpečnosť | Min. TPM 2.0 a Bezpečnostný tamper spínač na chassis servera |  |  |
| Napájanie | Redundantné napájacie zdroje vymeniteľné za chodu typu hot-swap |  |  |
| Ventilátory a chladenie | Vysoko-výkonné a za chodu vymeniteľné ventilátory typu hot-swap |  |  |
| Správa a monitoring | Formou vzdialenej grafickej KVM konzoly  Možnosť štartu, reštartu a vypnutia servera cez sieť LAN, nezávisle od OS  Manažment hardvéru vrátane možnosti nastavenia RAID úrovne lokálnych diskov.  Požadovaná podpora pre DMTF Redfish API.  Požadovaná možnosť vzdialenej správy aj prostredníctvom mobilných zariadení typu smartphone, PC alebo tablet pomocou HTML5.  Požadované funkcionality a prístup k aktualizáciám musia byť poskytované s časovo neobmedzeným licenčným pokrytím. |  |  |
| Predporuchová diagnostika | Predporuchová diagnostika procesorov, pamäťových modulov, RAID radičov, napájacích zdrojov, ventilátorov a HDD/SSD. |  |  |
| Záručné podmienky | 3 roky priamo od výrobcu zariadenia  Oprava poruchy najneskôr do 24h od nahlásenia, vrátane víkendov a sviatkov.  Servis bude poskytovaný v mieste inštalácie.  Nahlasovanie poruchy v režime 24x7.  Vrátane služby ponechania vadného disku zákazníkovi v prípade jeho poruchy. |  |  |

### Inštalácia a konfigurácia servera pre riadenie prístupov zo vzdialených sietí a konfigurácia softvéru pre pripojenie ku vzdialenej ploche

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Fyzická inštalácia servera | Zapojenie do rack-u  Pripojenie do siete  Inštalácia a aktualizácia servera |  |  |
| Inštalácia softvéru | Inštalácia komponentov riešenia  Hardening |  |  |
| Konfigurácia softvéru servera | Konfigurácia komponentov riešenia |  |  |
| Konfigurácia softvéru pre pripojenie ku vzdialenej ploche | Konfigurácia softvéru pre pripojenie ku vzdialenej ploche |  |  |

### Vypracovanie návrhu riešenia softvéru pre riadenie prístupov zo vzdialených sietí

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Vypracovanie návrhu riešenia | Popis funkcionalít, ktoré sa budú používať  Používané služby a komponenty  Návrh architektúry riešenia  Požiadavky na licencie – licenčný model, možnosti rozšírenia riešenia  Hardvérové požiadavky  Softvérové požiadavky  Požiadavky na komunikáciu (komunikačná matica)  Požiadavky na integráciu s infraštruktúrnymi službami (Active Directory, group policy a ďalšie)  Popis konfigurácie jednotlivých funkcií, služieb a komponentov  Zálohovanie a obnova systému, konfigurácie a údajov |  |  |

### Konfigurácia softvéru pre riadenie prístupov zo vzdialených sietí

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Konfigurácia softvéru | Konfigurácia komponentov riešenia v navrhnutej architektúre.  Integrácia s infraštruktúrnymi službami.  Konfigurácia používateľských kont a skupín.  Konfigurácia služieb, web portálu.  Implementácia/integrácia s 2FA.  Konfigurácia politík/platforiem.  Konfigurácia reportovania.  Konfigurácia zálohovania. |  |  |
| Minimálne požiadavky na konfiguráciu | Inštalácia komponentov v štandardnej dostupnosti (DR mode)  Integrácia do infraštruktúry (SMTP, SNMP, NTP, AD)  Integrácia s max. 30 cieľovými systémami Objednávateľa  Konfigurácia/integrácia s dvojfaktorovou autentizáciou 2FA  Implementácia a konfigurácia bezpečného vzdialeného prístupu cez web bránu a vybranú aplikáciu (napr. Putty)  Návrh a implementácia politík/platforiem  Vytvorenie používateľov a rolí, matice prístupov  Návrh a implementácia bezpečnostných a správcovských politík (vrátane výnimiek)  Príprava integrácie so SIEM  Integrácia na proces zálohovania a archivácie dát  Implementácia DR procesu (obnova po havárii)  Hardening komponentov |  |  |

### Overovanie a ladenie systému pre riadenie prístupov zo vzdialených sietí

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Overovanie a ladenie | Testovanie funkcionalít riešenia podľa vopred odsúhlasených testovacích scenárov  Test bezpečného pripojenia externého dodávateľa na cieľový systém |  |  |

### Vypracovanie dokumentácie riešenia systému pre riadenie prístupov zo vzdialených sietí

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Vypracovanie dokumentácie riešenia | Vypracovanie a dodanie projektovej dokumentácie v rozsahu: dokumentácia výrobcu, technická dokumentácia popisujúca skutočné vyhotovenie, používateľská príručka.  **Minimálne požiadavky na technickú dokumentáciu:**  Popis funkcionalít, ktoré sa používajú  Používané služby a komponenty  Popis architektúry riešenia a obrazová schéma  Používané licencie  Popis hardvérovej konfigurácie  Zoznam nainštalovaného softvéru  Popis komunikácie  Popis používaných infraštruktúrnych služieb (Active Directory, group policy a ďalšie)  Popis konfigurácie jednotlivých funkcií, služieb a komponentov  Popis zálohovania a obnovy riešenia, konfigurácie a dát |  |  |

### Zaškolenie administrátorov systému pre riadenie prístupov zo vzdialených sietí

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Zaškolenie administrátorov | Zaškolenie používateľov podľa rolí – správca riešenia, audítor, externý používateľ, interný používateľ.  Od základného zoznámenia so systémom až po jeho administráciu. |  |  |

## Virtualizačná platforma pre prevádzku bezpečnostných systémov

Virtualizačná platforma bude slúžiť pre vysoko dostupnú prevádzku serverov pre bezpečnostné systémy.

### Operačný systém servera virtualizačnej platformy + hypervízor

Údaje o ponúkanom zariadení/systéme:

Výrobca: <doplniť>

Model: <doplniť>

Konfigurácia: <doplniť detailnú konfiguráciu ponúkaného zariadenia/systému>

Odkaz na produktovú dokumentáciu na stránkach výrobcu (link): <doplniť link, kde je možné overiť parametre ponúkaných produktov>

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Počet podporovaných logických procesorov na host | Min. 512 |  |  |
| Podporovaná fyzická pamäť | Min. 4TB |  |  |
| Podporovaný počet virtuálnych CPU per host | Min. 2048 |  |  |
| Podporovaný počet virtuálnych serverov per host | Min. 1024 |  |  |
| Požadované vlastnosti | Vysoká dostupnosť (HA)  Fault tolerance (bezvýpadkové HA)  Lokálne a zdieľané úložiská  Podpora pre zálohovanie a obnovu  Podpora pre 10G Ethernet  Podpora VLAN  Vytváranie šablón  Migrácia virtuálnych serverov počas behu  Transparentné zdieľanie pamäte  RAM Overcommittment (presiahnutie veľkosti fyzickej RAM)  Rezervácia procesorového výkonu a pamäte  Podpora pre logické združovanie zdrojov pre rôzne skupiny (na základe príslušnosti k systému alebo oddeleniu) |  |  |
| Podporované operačné systémy virtuálnych serverov | Microsoft Windows, Linux |  |  |

### Server pre virtualizačnú platformu

V rámci dodávky riešenia požadujeme dodať 4 ks virtualizačných serverov s možnosťou ďalšieho pridania v prípade potreby.

Údaje o ponúkanom zariadení/systéme:

Výrobca: <doplniť>

Model: <doplniť>

Konfigurácia: <doplniť detailnú konfiguráciu ponúkaného zariadenia/systému>

Odkaz na produktovú dokumentáciu na stránkach výrobcu (link): <doplniť link, kde je možné overiť parametre ponúkaných produktov>

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Prevedenie | Optimalizovaný pre umiestnenie do 19" dátového rozvádzača (racku), výška max. 1U  Uchytenie servera v racku na výsuvných koľajniciach |  |  |
| Požiadavky na procesor(y) | Osadený minimálne jeden procesor s parametrami: min. 16 jadier.  Server musí byť preukázateľne schopný dosiahnuť výsledok v teste SPECrate®2017\_int\_base aspoň 160 bodov.  Údaj o výkone musí byť preukázateľný pre konkrétny ponúkaný server na verejne dostupnej stránke https://www.spec.org |  |  |
| Systémová pamäť | Server disponuje min. 16 využiteľnými pamäťovými slotmi, pamäť celkovo rozšíriteľná do min. 2TB  Osadená kapacita: min. 512GB DDR4 3200MHz Registered DIMM, s funkciou detekcie a opravy multibitových chýb, zrkadlenia pamätí, on-line spare pamäte |  |  |
| Subsystém pevných diskov | Server musí podporovať budúce rozšírenie interných pozícií pre 2,5" disky typu hot-swap do počtu min. 12 ks bez potreby pripojenia externej diskovej police.  Osadené 2x min. 480GB SATA SSD typu m.2 priamo na matičnej doske, nakonfigurované v RAID 1.  Min. prepisová kapacita 1324TB alebo min 1,5 DWPD. Minimálne výkonnostné parametre disku: 85tis IOPS pri čítaní (4kB bloky) a 36tis pri zápise (4kB bloky). |  |  |
| NVMe | Podpora NVMe diskov |  |  |
| Sieťové adaptéry | Min. 1x 2-portový 10/25Gbps ethernet adaptér pre pripojenie k externému prostrediu s rozhraním SFP+, adaptér typu onboard alebo ako PCIe rozširujúca karta  Min. 1x 2-portový 1Gbps ethernet adaptér pre pripojenie k externému prostrediu metalickým rozhraním typu RJ45  Dedikovaný port pre manažment servera |  |  |
| FibreChannel adaptér | Min. 1x dual port 16Gbps Fibre Channel adaptér vrátane príslušných prevodníkov |  |  |
| Dátové a video konektory | Min. 1x USB na prednom paneli  Min. 1x USB na pripojenie mobilného zariadenia typu smartfón alebo tablet pre použite manažovacej aplikácie za účelom fyzického servisovania zariadenia  Min. 2x USB porty a 1x VGA port na zadnom paneli |  |  |
| Rozširujúce sloty | Min. 2x PCIe x16 gen4 s možnosťou rozšírenia o ďalší PCIe x16 slot. |  |  |
| Bezpečnosť | Min. TPM 2.0 a Bezpečnostný tamper spínač na chassis servera |  |  |
| Napájanie | Redundantné napájacie zdroje vymeniteľné za chodu typu hot-swap |  |  |
| Ventilátory a chladenie | Vysoko-výkonné a za chodu vymeniteľné ventilátory typu hot-swap |  |  |
| Správa a monitoring | Formou vzdialenej grafickej KVM konzoly  Možnosť štartu, reštartu a vypnutia servera cez sieť LAN, nezávisle od OS  Manažment hardvéru vrátane možnosti nastavenia RAID úrovne lokálnych diskov.  Požadovaná podpora pre DMTF Redfish API.  Požadovaná možnosť vzdialenej správy aj prostredníctvom mobilných zariadení typu smartphone, PC alebo tablet pomocou HTML5.  Požadované funkcionality a prístup k aktualizáciám musia byť poskytované s časovo neobmedzeným licenčným pokrytím. |  |  |
| Operačný systém | Microsoft Windows Server 2019  Licencie pre všetky jadrá osadených CPU  Licenčné pokrytie pre neobmedzený počet virtuálnych serverov |  |  |
| Predporuchová diagnostika | Predporuchová diagnostika procesorov, pamäťových modulov, RAID radičov, napájacích zdrojov, ventilátorov a HDD/SSD. |  |  |
| Záručné podmienky | 3 roky priamo od výrobcu zariadenia  Oprava poruchy najneskôr do 24h od nahlásenia, vrátane víkendov a sviatkov.  Servis bude poskytovaný v mieste inštalácie.  Nahlasovanie poruchy v režime 24x7.  Vrátane služby ponechania vadného disku zákazníkovi v prípade jeho poruchy. |  |  |

### Rack s príslušenstvom pre virtualizačnú platformu

Údaje o ponúkanom zariadení/systéme:

Výrobca: <doplniť>

Model: <doplniť>

Konfigurácia: <doplniť detailnú konfiguráciu ponúkaného zariadenia/systému>

Odkaz na produktovú dokumentáciu na stránkach výrobcu (link): <doplniť link, kde je možné overiť parametre ponúkaných produktov>

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Prevedenie | Štandardná dátová skriňa (rack) šírky 19“ s výškou 42U |  |  |
| Príslušenstvo | Stabilizačné prvky, bočné panely  Konzola pre obsluhu (monitor, klávesnica, myš)  Súčasťou dodávky musia byť aj všetky potrebné káble a súprava na montáž |  |  |
| Záručné podmienky | Záruka 3 roky s dobou odozvy v najbližší pracovný deň |  |  |

### Switch 10Gbit pre virtualizačnú platformu

10 Gbit prepínače budú tvoriť vysokorýchlostnú sieť LAN na prepojenie komponentov virtualizačnej platformy a na pripojenie zálohovacieho systému. Požadujeme použitie 2ks prepínačov na zabezpečenie redundancie, pričom všetky zariadenia musia byť pripojené do každého z týchto prepínačov.

Údaje o ponúkanom zariadení/systéme:

Výrobca: <doplniť>

Model: <doplniť>

Konfigurácia: <doplniť detailnú konfiguráciu ponúkaného zariadenia/systému>

Odkaz na produktovú dokumentáciu na stránkach výrobcu (link): <doplniť link, kde je možné overiť parametre ponúkaných produktov>

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Typ zariadenia | Sieťový repínač s modulárnymi šachtami minimálne pre moduly 1000 SFP / 10000 SFP+ |  |  |
| Počet portov | Minimálne 16 |  |  |
| Prevedenie | Montovateľné do štandardnej dátovej skrine so šírkou 19“  Maximálna výška 1U |  |  |
| Priepustnosť | Min. 255 Mpps (64-byte packety) |  |  |
| Prepínacia kapacita | Min. 450 Gbps |  |  |
| Napájanie | Minimálne 2x redundantný napájací zdroj vymeniteľný za chodu |  |  |
| Požadovaná funkcionalita | Podpora stohovania (stack) zariadení až do 8ks  Stohovaná konfigurácia, prepojenie min. 2x40 Gbit/s  RJ-45 Out-of-Band Management rozhranie  REST API pre funkcionality automatizácie, scriptovania  Podpora funkcionality QoS, CoS, IEEE 802.1ad QinQ, IEEE 802.3ad Link Aggregation Protocol (LACP) |  |  |
| Záručné podmienky | 3 roky, NBD (Next Business Day) |  |  |

### Switch 1 Gbit pre virtualizačnú platformu

1 Gbit prepínače budú slúžiť na pripojenie management rozhraní všetkých zariadení ako aj na oddelenie sietí s nižšími požiadavkami na šírku pásma (napr. DMZ) v rámci virtualizačnej platformy a internú klastrovú komunikáciu. Požadujeme použitie 2 ks prepínačov na každej lokalite (celkovo 4 ks), pričom tam, kde je to možné, budú zariadenia pripojené do oboch zariadení (okrem management portov, ktoré to neumožňujú).

Údaje o ponúkanom zariadení/systéme:

Výrobca: <doplniť>

Model: <doplniť>

Konfigurácia: <doplniť detailnú konfiguráciu ponúkaného zariadenia/systému>

Odkaz na produktovú dokumentáciu na stránkach výrobcu (link): <doplniť link, kde je možné overiť parametre ponúkaných produktov>

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Typ zariadenia | Sieťový prepínač s podporou Autosensing 10/100/1000 RJ-45 metalickými rozhraniami |  |  |
| Počet portov | Minimálne 24 |  |  |
| Prevedenie | Montovateľné do štandardnej dátovej skrine so šírkou 19“  Maximálna výška 1U |  |  |
| Priepustnosť | Min. 90 Mpps (64-byte packety) |  |  |
| Prepínacia kapacita | Min. 120 Gbps |  |  |
| Napájanie | Minimálne 2x redundantný napájací zdroj vymeniteľný za chodu |  |  |
| Požadovaná funkcionalita | Podpora stohovania (stack) zariadení až do 8ks  RJ-45 Out-of-Band Management rozhranie  REST API pre funkcionality automatizácie, scriptovania  Podpora funkcionality QoS, CoS, IEEE 802.1ad QinQ, IEEE 802.3ad Link Aggregation Protocol (LACP) |  |  |
| Záručné podmienky | 3 roky, NBD (Next Business Day) |  |  |

### Diskové pole pre virtualizačnú platformu

Údaje o ponúkanom zariadení/systéme:

Výrobca: <doplniť>

Model: <doplniť>

Konfigurácia: <doplniť detailnú konfiguráciu ponúkaného zariadenia/systému>

Odkaz na produktovú dokumentáciu na stránkach výrobcu (link): <doplniť link, kde je možné overiť parametre ponúkaných produktov>

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Kapacita | Minimálna využiteľná kapacita 50TB s využitím distribuovaného RAID6. |  |  |
| Použité disky | NVMe Flash/SSD diskové moduly s hardvérovou in-line kompresiou a šifrovaním dát |  |  |
| Prevedenie | End-to-end NVMe diskové pole o celkovej veľkosti max. 2RU montovateľné do štandardnej dátovej skrine |  |  |
| Redundancia | Redundantné kontroléry v režime active-active  Redundantné napájacie zdroje vymeniteľné za chodu |  |  |
| Rozšíriteľnosť | Systém umožňuje v budúcnosti ďalšie rozširovanie fyzickej kapacity minimálne na 2-násobok prvotne osadeného počtu diskov |  |  |
| Podpora RAID | Podpora RAID 1, 5, 6, pričom „hot spare“ priestor je distribuovaný cez všetky diskové moduly v RAID skupine (nie dedikovaný globálny hot spare disk)  Umožňuje online rozšírenie RAID skupiny pridaním len jedného disku (bez prerušenia chodu aplikácií). Minimálnym krokom pri rozšírení kapacity je 1 disk |  |  |
| Podporované typy diskov | NVMe Flash/SSD diskové moduly s in-line HW kompresiou a šifrovaním  SSD NVMe  SCM NVMe  SSD SAS  10k RPM SAS HDD  7k2 RPM NL SAS HDD |  |  |
| Údržba za chodu | Online upgrade mikrokódov kontrolérov, flash/SSD modulov a rotačných diskov a online výmena kľúčových komponentov diskového poľa |  |  |
| Replikácia | Umožňuje dátovú replikáciu pre požadovanú kapacitu v synchrónnom a asynchrónnom móde medzi dvoma až troma lokalitami s časovo neobmedzeným licenčným pokrytím na požadovanú kapacitu |  |  |
| Host konektivita | Požadujeme pripojenie pomocou Fibre Channel, minimálne 16 Gbit/s  Podpora pre 16Gb/s FC, 32Gb/s FC, 10GbE iSCSI, SAS, 25Gb/s iSER iSCSI  Požadujeme redundantné pripojenie, min. 4 porty pre každý radič |  |  |
| Vyrovnávacia pamäť | Vyrovnávacia systémová pamäť cache minimálne 512 GB (nie flash cache) |  |  |
| Podpora SSD/Flash modulov | Požadujeme počas obdobia HW servisnej podpory garanciu výmeny Flash/SSD modulov v prípade ich výpadku bez ohľadu na počet prepisov ich RAW kapacity v čase vzniku poruchy |  |  |
| Rozšírené funkcie | Umožňuje virtualizáciu internej diskovej kapacity a thin provisioning s časovo neobmedzeným licenčným pokrytím na požadovanú kapacitu  Umožňuje automatický load balancing LUN –ov v rámci single tierového storage poolu (optimalizácia rozloženia záťaže)  Umožňuje vytváranie lokálnych kópii dát (snapshot-ov a klonov) s časovo neobmedzeným licenčným pokrytím na požadovanú kapacitu  Umožňuje kombináciu viacerých druhov rotačných/SSD/Flash diskových modulov rovnakého fyzického prevedenia, ale rôznych kapacít, prípadne výkonových parametrov v rámci jedného kontroléra alebo jednej diskovej police  Umožňuje klastrovanie systémov  Podporuje virtualizáciu externých diskových polí od rôznych výrobcov  Umožňuje SW kompresiu a deduplikáciu s časovo neobmedzeným licenčným pokrytím na požadovanú kapacitu  Podporuje „data at rest“ šifrovanie dát  Podporuje HW kompresiu a šifrovanie dát pri Flash/SSD moduloch bez zaťažovania CPU kontrolérov  Umožňuje automatický tiering na báze umelej inteligencie, synchrónnu a asynchrónnu replikáciu dát medzi dvomi až tromi lokalitami  Obsahuje integrovaný migračný nastroj na migráciu dát s diskových polí aj od iných výrobcov s časovo neobmedzeným licenčným pokrytím na požadovanú kapacitu |  |  |
| Správa diskového poľa | Podpora SNMP, e-mail notifikácia a podpora call-home  Diskové pole musí obsahovať GUI prostredníctvom HTTPS, CLI prostredníctvom SSHv2 a všetky potrebné multipath ovládače pre požadované podporované OS  Podporuje RESTfull Api a CSI  Navrhované diskové pole musí umožňovať pripojenie ku cloudovej službe výrobcu diskového poľa a musí umožňovať monitoring výkonu, kapacity a proaktívny monitoring navrhovaného diskového poľa. Uvedená cloudová služba musí podporovať automatizáciu procesu servisnej podpory s cieľom dosiahnutia rýchlejšieho riešenia HW a SW problémov (ako napr. automatická kolekcia logov, filtrovanie udalostí, vytváranie a manažment servisných ticketov) |  |  |
| Záručné podmienky | SW a HW podpora na obdobie 3 rokov s pokrytím 24x7 a garantovanou dobou odstránenia poruchy najbližší pracovný deň |  |  |
| SAN prepínače | Súčasťou dodávky diskového poľa musia byť aj 2ks Fibre Channel SAN prepínačov s nasledujúcimi parametrami:  Optimalizovaný na umiestnenie do 19“ rackovej skrine, výška max. 1U  Celkový počet portov min. 24x 8/16/32Gbps FC  Aktívny počet portov min. 16x 16Gbps FC vrátane príslušných SFP+ transceiverov  Podpora pre Full Fabric mode: F\_Port, M\_Port (Mirror Port), E\_Port, D\_Port (Diagnostic Port)  Podpora pre Access Gateway mode: F\_Port and NPIV-enabled N\_Port  Záruka 3 roky v mieste inštalácie, 24x7 s dobou odozvy do 4h od nahlásenia poruchy |  |  |

### Kabeláž LAN/SAN pre virtualizačnú platformu

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Kabeláž | Predmetom dodávky musí byť všetka kabeláž potrebná na inštaláciu, zapojenie a oživenie riešenia v rámci dodávanej dátovej skrine.  Kabeláž potrebnú na pripojenie riešenia do existujúcej infraštruktúry vrátane prípravy napájacích prívodov zabezpečí Objednávateľ. |  |  |

### Inštalácia HW a systémového prostredia

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Vypracovanie detailného návrhu virtualizačnej platformy | Analýza požiadaviek  Návrh architektúry a konfigurácie virtualizačnej platformy  Návrh konfigurácie diskových priestorov  Návrh konfigurácie sietí  Návrh postupov pre vytváranie a konfiguráciu virtuálnych serverov  Návrh pracovných postupov pre údržbu systému |  |  |
| Fyzická inštalácia dátovej skrine (racku) – v 2 lokalitách | Kompletizácia racku  Umiestnenie na určené miesto, stabilizácia  Fyzická montáž záložného zdroja  Pripojenie racku na napájanie  Konfigurácia záložného zdroja a PDU v racku |  |  |
| Inštalácia a konfigurácia sieťových komponentov LAN – 2 lokality | Fyzická inštalácia komponentov do racku  Pripojenie napájania  Aktualizácia mikrokódov  Konfigurácia prepojenia prepínačov do stacku  Pripojenie siete do existujúcej infraštruktúry Objednávateľa  Test lokálnej konektivity, test konektivity do internetu  Diagnostika, kontrola logov |  |  |
| Inštalácia a konfigurácia SAN siete – 1 lokalita | Fyzická inštalácia komponentov do racku  Pripojenie napájania  Aktualizácia mikrokódov  Konfigurácia pripojenia zariadení do management siete  Zónovanie SAN siete  Diagnostika, kontrola logov |  |  |
| Inštalácia a konfigurácia serverov – 1 lokalita | Fyzická inštalácia serverov do dátovej skrine (racku)  Zapojenie kabeláže pre napájanie a sieťovú konektivitu (LAN, SAN)  Konfigurácia management rozhrania serverov  Aktualizácia mikrokódov servera a interných komponentov na verzie odporúčané výrobcom zariadení  Diagnostika, kontrola logov |  |  |
| Inštalácia a konfigurácia diskového poľa - 1 lokalita | Fyzická inštalácia diskového poľa do racku  Pripojenie napájania  Konfigurácia pripojenia zariadení do management siete  Aktualizácia mikrokódov  Vytvorenie RAID zväzkov a logických diskov  Pripojenie do siete SAN  Diagnostika, kontrola logov |  |  |
| Inštalácia a konfigurácia virtualizačnej platformy | Inštalácia a konfigurácia hypervízora na všetky fyzické servery  Inštalácia a konfigurácia managementu virtualizačnej platformy  Aktualizácia verzií hypervízora a jednotlivých ovládačov  Konfigurácia používateľov a prístupových práv  Pripojenie zdieľaných diskových úložísk  Vytvorenie šablón virtuálnych serverov  Vytvorenie virtuálnych serverov podľa požiadaviek Objednávateľa |  |  |
| Test systémového prostredia | Test sieťovej konektivity  Test zabezpečenia vysokej dostupnosti (online migrácia virtuálnych serverov) |  |  |
| Zaškolenie obsluhy | Zaškolenie v dĺžke trvania 1 deň pre ľubovoľný počet administrátorov v priestoroch Objednávateľa |  |  |

### Monitorovací systém

V rámci dodávky riešenia požadujeme navrhnúť a implementovať monitorovací systém s cieľom monitorovania všetkých hardvérových komponentov dodaného riešenia z pohľadu dostupnosti, kapacitných a výkonnostných parametrov s možnosťou rozšírenia na ďalšie systémy a služby Objednávateľa.

Údaje o ponúkanom zariadení/systéme:

Výrobca: <doplniť>

Model: <doplniť>

Konfigurácia: <doplniť detailnú konfiguráciu ponúkaného zariadenia/systému>

Odkaz na produktovú dokumentáciu na stránkach výrobcu (link): <doplniť link, kde je možné overiť parametre ponúkaných produktov>

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Vlastnosti monitorovacieho systému | Monitorovanie fyzických zariadení (sieťové prepínače, záložné zdroje, servery, diskové polia, pásková knižnica) na úrovni dostupnosti  Monitorovanie dodanej virtualizačnej platformy na úrovni dostupnosti, kapacity a výkonnostných parametrov  Monitorovanie operačných systémov fyzických a virtuálnych serverov – pri serveroch je požadované monitorovanie min. CPU, RAM, diskových priestorov a event logov  Možnosť definovania vlastných prahových hodnôt pre notifikácie  Možnosť vytvárania vlastných obrazoviek a dashboardov pre jednotlivých používateľov ako aj centrálne definovanie predvolených obrazoviek  Možnosť monitorovania webových stránok a sekvencií webových stránok so simuláciou práce používateľa  Možnosť zasielania e-mailových notifikácií pri dosiahnutí alebo prekročení nastavených prahových hodnôt  Webová konzola pre používateľov |  |  |
| Rozsah nasadenia | Všetky dodané HW zariadenia  Operačné systémy všetkých dodaných fyzických serverov  Operačné systémy neobmedzeného počtu virtuálnych serverov  Virtualizačná platforma  Licenčné pokrytie pre neobmedzený počet používateľov  Implementácia bez nutnosti samostatného fyzického servera (napríklad ako virtuálny server v rámci virtualizačnej platformy) |  |  |
| Požadované služby | Detailný návrh monitorovacieho systému  Inštalácia a konfigurácia riešenia  Konfigurácia monitorovania všetkých dodaných HW zariadení a virtualizačnej platformy  Konfigurácia zasielania notifikácií  Konfigurácia prahových hodnôt a notifikácií na základe odporúčaní (Best practice)  Príprava štandardných obrazoviek a dashboardov pre jednotlivé skupiny používateľov  Vypracovanie prevádzkovej dokumentácie s uvedením prevádzkových postupov pre pridávanie nových systémov do monitorovacieho systému a pre správu a údržbu systému  Zaškolenie obsluhy v trvaní 1 deň pre ľubovoľný počet používateľov v priestoroch Objednávateľa |  |  |

### Helpdesk systém

V rámci dodávky riešenia požadujeme navrhnúť a implementovať helpdesk systém s cieľom evidencie incidentov a chybových hlásení súvisiacich s prevádzkou dodaného riešenia, hlásením incidentov poskytovateľom prevádzkovej podpory a s možnosťou rozšírenia na ďalšie systémy a služby Objednávateľa.

Údaje o ponúkanom zariadení/systéme:

Výrobca: <doplniť>

Model: <doplniť>

Konfigurácia: <doplniť detailnú konfiguráciu ponúkaného zariadenia/systému>

Odkaz na produktovú dokumentáciu na stránkach výrobcu (link): <doplniť link, kde je možné overiť parametre ponúkaných produktov>

Požadované parametre

| Parameter | Špecifikácia (min. parametre) | Splnenie požiadaviek [áno/nie] | Hodnota parametra |
| --- | --- | --- | --- |
| Vlastnosti helpdesk systému | Evidencia servisných požiadaviek (ticketov) súvisiacich s prevádzkou dodaného riešenia  Možnosť vytvárania skupín riešiteľov podľa oblasti zodpovednosti  Webové rozhranie na zadávanie požiadaviek  Webové rozhranie pre riešiteľov  Ukladanie všetkých požiadaviek v relačnej databáze  Možnosť pridávania príloh k jednotlivým požiadavkám  Ukladanie histórie priebehu riešenia jednotlivých požiadaviek  Možnosť delegácie riešenia na podporu vyššej úrovne, resp. na dodávateľa prevádzkovej podpory mimo organizácie Objednávateľa  Možnosť zasielania notifikácií pri zmene stavu riešenej požiadavky  Podpora pre akceptovanie/odmietnutie riešenia požiadavky  Možnosť tvorby znalostnej bázy pre riešiteľov  Možnosť nastavenia rôznych úrovní závažnosti požiadaviek  Možnosť definovania rôznej úrovne služby pre jednotlivé systémy  Možnosť rozšírenia systému na ďalšie systémy a služby prevádzkované Objednávateľom |  |  |
| Rozsah nasadenia | Vytvorenie dátových štruktúr pre všetky dodané subsystémy riešenia (Hardvér, Softvér, Virtualizačná platforma, zálohovací systém, podporné systémy)  Licenčné pokrytie pre neobmedzený počet používateľov (zadávateľov)  Licenčné pokrytie pre minimálne 5 interných a 5 externých riešiteľov  Implementácia bez nutnosti samostatného fyzického servera (napríklad ako virtuálny server v rámci virtualizačnej platformy) |  |  |
| Požadované služby | Detailný návrh helpdesk systému  Inštalácia a konfigurácia riešenia  Konfigurácia zasielania notifikácií  Konfigurácia používateľov a prístupových práv  Vytvorenie dátových štruktúr pre všetky dodané subsystémy riešenia (Hardvér, Softvér, Virtualizačná platforma, zálohovací systém, podporné systémy)  Príprava štandardných reportov a štatistík (počet požiadaviek, počet otvorených požiadaviek, počet vyriešených požiadaviek, počet požiadaviek riešených prostredníctvom externých riešiteľov, najúspešnejší riešitelia, najmenej úspešní riešitelia)  Vypracovanie prevádzkovej dokumentácie s uvedením prevádzkových postupov pre pridávanie nových systémov do helpdesk systému a pre správu a údržbu systému  Zaškolenie obsluhy v trvaní 1 deň pre ľubovoľný počet používateľov v priestoroch Objednávateľa |  |  |

|  |  |
| --- | --- |
| V ........................., dňa ............... | .............................................................  meno a priezvisko, funkcia  podpis[[1]](#footnote-1)1 |

1. 1 Doklad musí byť podpísaný uchádzačom, jeho štatutárnym orgánom alebo členom štatutárneho orgánu alebo iným zástupcom uchádzača, ktorý je oprávnený konať v mene uchádzača v obchodných záväzkových vzťahoch. [↑](#footnote-ref-1)