OPIS PREDMETU ZÁKAZKY

Názov zákazky:
Riadenie kybernetickej bezpečnosti – Kontrola prístupu zariadení do siete

Verejný obstarávateľ prevádzkuje svoju činnosť vo viacerých lokalitách v rámci Slovenskej republiky. Jednotlivé pracoviská sú prepojené dátovou sieťou WAN, prostredníctvom ktorej zamestnanci pristupujú k aplikáciám, výpočtovým, informačným a komunikačným, zdrojom. V rámci celkového zvýšenia kybernetickej bezpečnosti organizácie je zámerom verejného obstarávateľa, nasadiť, rozšíriť prípadne doplniť systémy, prostredníctvom ktorých je možné spravovať, riadiť a kontrolovať zariadenia pristupujúce do siete verejného obstarávateľa.

A. Kontrola prístupu zariadení

Požadujeme návrh a dodanie riešenia a dodávku potrebných SW komponentov, resp. licencií a odborných služieb pre nasadenie overenia prístupu (NAC) do počítačovej siete pomocou štandardu 802.1x v prostredí verejného obstarávateľa.

Riadenie prístupu sa týka drôtovej časti siete, ale musí byť pripravené na možnú integráciu s nasadenou bezdrôtovou infraštruktúrou.

Celkovo sa jedná o nasadenie na nasledovných pracoviskách:

- 6 lokalít v Bratislave
- 8 krajských lokalít v sídlach krajov SR
- 53 okresných lokalít v rámci SR

Jedná sa o 152 ks prepínačov Cisco, prevažne rady Catalyst, a celkový počet 2300 koncových staníc.

Riešenie musí spĺňať nasledovné požiadavky

- Integrácia s existujúcou infraštruktúrou
- Umožňuje správcom siete spravovať a kontrolovať prístup k sieťovým zariadeniam na základe ich rolí a úrovne oprávnení
- Umožňuje zabezpečiť bezpečný prístup hostí do siete a zároveň zabezpečiť, aby mali hosťujúci používatelia obmedzený a kontrolovaný prístup k sieťovým zdrojom
- Umožňuje automaticky identifikovať a klasifikovať sieťové zariadenia na základe ich typu, operačného systému a ďalších atribútov, tzv. profiling.
- Umožňuje automaticky identifikovať a klasifikovať sieťové zariadenia na základe ich typu, operačného systému a ďalších atribútov
- Umožňuje správcom presadzovať zásady zabezpečenia a zhody zariadení, napríklad zabezpečiť, aby zariadenia mali aktualizovaný antivírusový softvér alebo aby na nich boli nainštalované najnovšie záplaty operačného systému
- Umožňuje overovať a autorizovať používateľov siete na základe ich používateľského mena a hesla.
- Umožňuje správcom riadiť prístup do siete na základe identity používateľa a/alebo typu zariadenia
- Definovanie a presadzovanie zásad prístupu k sieti, ako je napríklad riadenie prístupu k určitým aplikáciám alebo službám.
- Centralizovaná správu identít a poverení používateľov vrátane integrácie s externými zdrojmi identít, ako je Active Directory alebo LDAP.

- Monitorovanie sieťovej aktivity a vytváranie správ o prístupe k sieti, dodržiavaní predpisov a ďalších ukazovateľoch.
- Vyžadovanie ďalších foriem overovania okrem používateľského mena a hesla, ako napríklad čipovú kartu alebo biometrické overovanie.

- všade, kde je to možné bol využívaný štandardný suplikant (Win OS, macOS, Xerox...)
- zariadenia, ktoré nemajú natívneho 802.1x suplikanta budú využívať MAB autentifikáciu
- podpora využívania internej databázy užívateľov a zariadení
- Riešenie musí umožňovať definovať skupinu MAC adries podľa výrobcov
- riešenie musí podporovať pravidelne aktualizovanú databázu MAC adries

Rozsah dodaných služieb

Ako súčasť dodávky požaduje verejný obstarávateľ realizáciu analytických, inštalačných a konfiguračných služieb na zabezpečenie implementácie a otestovanie funkčnosti štandardu 802.1x v prostredí verejného obstarávateľa, vrátane:

- Analýzy IKT prostredia verejného obstarávateľa a funkčný návrh riešenia
- Inštalácie a inicializácie SW komponentov riešenia
- Aktualizácia súčasných AAA serverov na aktuálnu, podporovanú verziu
- Zabezpečenie zmeny licencovania v súlade s nasadením aktuálnej verzie riešenia
- Implementácia on-premise servera na správu licencií
- Konfigurácie AAA
- Konfigurácie PC suplikant policy
- Konfigurácie PKI
- Konfigurácia switchov
- Testovania a ladenia
- Projektový manažment a riadenie projektu
- Dokumentácia

Dodávateľ zabezpečí aj nasledovné aktivity:

Riadenie projektu

- Na strane dodávateľa bude definovaný PM, ktorý bude zabezpečovať koordináciu aktivít dodania projektu
- V rámci projektu bude vedená evidencia požadovaných, realizovaných, ako aj otvorených úloh

Analýza a Dizajn

Dodávateľ je zodpovedný za oboznámenie sa s prostredím, do ktorého bude navrhované riešenie inštalované, a to :

- oboznámenie sa s aktuálnymi nastaveniami a topológiou
- vypracovanie návrh implementačného konceptu na základe rozsahu a požadovaných vlastností riešenia

Inštalácia

Inštalácia bude realizovaná v niekoľkých krokoch:

- aktualizácia AAA serverov a aktualizácia licenčného modelu (vrátane licenčného servera)
- Nasadenie riešenia v testovacom labe, kde budú preverené všetky požadované funkcionality (802.1x, MAB..) riešenia na rôznom sieťovom HW využívanom v prostredí verejného obstarávateľa
- Nasadenie na zvolenú KP a OP

- Postupné nasadenia na všetky krajské a okresné pracoviská, s on-site prítomnosťou v čase migrácie

Dokumentácia

- Dodávateľ dodá implementačný postup (LLD)
- Ďalej dodá systémovú dokumentáciu k dodanému riešeniu
- Po implementačnú dokumentáciu, ktorá musí obsahovať minimálne nasledujúce časti:
    - architektúru riešenia a popis systému pre administrátorov
    - aktualizácia dizajn dokumentu podľa realizácie - zodpovedajúci stavu v termíne odovzdania
    - backup / restore procedúry