**Příloha č. 1 – Podrobná specifikace Díla**

Cílem technického řešení je zvýšení bezpečnosti přístupových portů LAN switchů v lokalitách Objednatele. Primárním účelem je ochrana proti neoprávněnému připojení koncových zařízení do fyzické datové infrastruktury Objednatele a následný přístup k interním zdrojům. Implementace 802.1X Zhotovitelem na aktuálně provozovaných síťových prvcích Arista, které umožní řídit přístup k drátové síti LAN a také k bezdrátové síti WLAN.

##  *Předplatné licencí*

Rozšíření řešení ARISTA CloudVision o část AGNI (ARISTA Next Generation Identity/Access). AGNI je platforma pro automatizaci a správu sítí, zaměřená na automatizaci síťových operací, zjednodušení nasazení infrastruktury a optimalizaci provozu v souvislosti s využitím 802.1X.

Zhotovitel zajistí dodání ročního předplatného licence v rozsahu 1000 zařízení.

Předplatné bude dodáno a aktivováno až při započetí implementačních prací.

1. ***Implementační a konfigurační práce***

**Implementace 802.1X**

Jedná se o bezpečnostní technologii, kdy dochází k ověřování uživatelů, kteří se pokoušejí o přístup do interní sítě – připojení k fyzické infrastruktuře. K autentizací bude sloužit certifikát interní certifikační autority. Samotné ověření bude probíhat na AUTHENTICATION serveru, kde tuto roli bude plnit doménový controller AD. Jelikož ne všechna koncová zařízení podporují ověřování pomocí 802.1X, budou vyžity následující dva scénáře:

* Klienti podporující 802.1X (PC, notebooky, atd.)
* po připojení dojde k ověření pomocí certifikátu zařízení
* Klienti nepodporující 802.1X (tiskárny, IP telefony, dveřníky, obecně IoT)
* Pro zajištění řízení přístupů do interní sítě, bude využito technologie MAB (MAC Authentication Bypass). Tedy pokud se k přístupovému portu připojí zařízení nepodporující 802.1X, tak dojde k autentizaci pomoci fyzické MAC adresy zařízení.

**Postup implementace**

* Nasazení technologie Arista AGNI, vycházející ze standardizovaného protokolu IEEE 802.1X, který definuje autentizaci a autorizaci uživatele nebo zařízení
* Navržení a pilotní nasazení řešení ověřování koncových stanic uživatelů a jiných zařízení před jejich plným připojením do LAN prostřednictvím přístupových přepínačů.
* Naimplementování interní certifikační autority a schopnost zajištění vydávání certifikátů v součinnosti se správcem AD
* Zajištění funkčnosti neinteraktivních zařízení, jako jsou např. síťové tiskárny nebo zařízení třetích stran připojené do LAN prostřednictvím přístupových přepínačů
* Zajištění vazby řešení na stávající zdroje (databáze) informací o uživatelích a jejich právech (Active Directory)
* Pilotní ověření bezpečnostního auditu zařízení (tzv. posture assessment) na vybraných stanicích interních i externích uživatelů (=uživatelů připojených přes VPN)
* Konfigurace autentizátorů (přístupových přepínačů) v lokalitách Objednatele
* Definice autentizačních a autorizačních pravidel
* Popis způsobu pilotního ověření na vybraných koncových stanicích a jiných vybraných zařízeních z LAN
* Pilotní ověření na vybraných koncových stanicích a jiných vybraných zařízení z LAN
* Pilotní nasazení na stanice uživatelů a další zařízení v pilotní lokalitě
* Akceptační testy – jak pro pilotní ověření, tak pro pilotní nasazení v LAN
* Plošné nasazení
* Vytvoření konfigurační a provozní dokumentace 802.1X a předání Objednateli
* Akceptační a předávací protokol

**Objednatel zajistí potřebnou součinnost:**

* Odsouhlasení návrhu řešení
* Spolupráce při návrhu – definice autentizačních a autorizačních politik
* Spolupráce při realizaci – zajištění vybraných koncových stanic a síťových zařízení pro jednotlivé etapy
* Součinnost při realizaci – zajištění interní certifikační autority
* Součinnost správců serverů, stanic, domény
* Dodání seznamu MAC adres zařízení nepodporujících 802.1X připojených do datové sítě v dotčených lokalitách
* Součinnost při provádění akceptačních testů