VZ20/2009
„Modernizace TS se zaměřením na dostupnost a bezpečnost“

Dodatečné informace k ZD

Otázka č. 1
Dotaz k bodu 9.2.6.2.e) Zadávací dokumentace:
"Jakou odbornost požaduje zadavatel od uchazeče předložit pro technologie jednotlivých stávajících systémů zadavatele, resp. o jaké stávající technologie a stávající systémy se jedná?"

Odpověď
Uchazeč musí prokázat odbornost pro technologie jednotlivých stávajících systémů zadavatele, u kterých bude provádět změny konfigurace nebo vytvoření vazby nutné z důvodu provedení implementace nabízeného technického řešení. Popis stávajících systémů je uveden v ZD Technická specifikace bod 1.4 Popis současného stavu a dále v bodě 3. Integrace TS ke stávajícím systémům.

Otázka č. 2
2. otázka
Zadavatel požaduje kryptaci provozu mezi AP a centrem pomocí dedikovaného speciálního HW zařízení. Vyžaduje zadavatele podporu kryptování veškerého datového provozu (tj. řídícího i datového) mezi AP a centrem nebo postačí kryptování pouze řídícího provozu pro správu AP s tím, že vlastní datový provoz (od a k bezdrátovým klientům do/z pevné sítě) bude přenášen nekryptovaně?

Odpověď
Zadavatele vyžaduje podporu kryptování veškerého datového provozu (tj. řídícího i datového) mezi AP a centrem.

Otázka č. 3
Zadavatel požaduje možnost na vyžádání přesně lokalizovat a zobrazit na mapě vybraného WiFi klienta nebo cizí AP. Postačí zadavateli možnost přesně lokalizovat v jeden okamžik pouze jednoho klienta nebo jednoho cizí AP v reálném čase nebo požaduje možnost přesně lokalizovat v reálném čase současně více klientů/cizích AP případně aktivních RFID tagů včetně ukládání historie záznamů o lokalizačních údajích po určitou dobu (pokud ano, tak pro jaký počet WLAN klientů a jaký počet aktivních RFID tagů)?

Odpověď
Zadavateli postačuje možnost přesně lokalizovat v jeden okamžik pouze jednoho klienta nebo jednoho cizí AP v reálném čase.

Otázka č. 4
Zadavatel požaduje IPS funkce pro WLAN sítě, s podporou detekce útoků na L2. Postačí zadavateli běžná funkcionalita nebo vyžaduje zadavatel i pokročilou detekci útoků na WLAN síť prováděnou na dedikovaných AP (neobsluhujících klienty) s možností proaktivní reakce včetně zachycení celého útoku pro forenzní analýzu, detekci anomálií pro neznámé útoky, znalostní bázi s popisem jednotlivých útoků, dlouhodobé ukládání záznamů o útocích a generování reportů (pokud ano, tak pro jaký počet AP je požadována pokročilá detekce)?

Odpověď
Všechna poptávaná AP budou sloužit k připojování WiFi klientů. Zadavatel neuvažuje o vyčlenění žádných AP pro IPS funkce.

Otázka č. 5
Požaduje zadavatel dodat k jednotlivým AP i antény? Pokud ano, tak jaký počet a s jakými parametry (zisk, směrová charakteristika, délka anténního kabelu)?

Odpověď
Uchazeč nabídne AP s interní anténou. Případná změna se bude řešit v průběhu realizace projektu.

Otázka č. 6

V dodatečných informacích k ZD je uvedeno, že „Uchazeč nabídne AP s interní anténou. Případná změna se bude řešit v průběhu realizace projektu.“, ale v technické specifikaci v příloze v bodu Accesspointy uvádíte požadavek na „Možnost připojení externí antény“. Požadavek na kombinaci interní antény se současným připojením antény externí je dle názoru uchazeče samoúčelný a omezuje výběr typu zařízení Accesspointů prakticky na jediného výrobce. Akceptuje zadavatel v tom případě návrh zařízení pouze s interní anténou a jeho případnou následnou změnu na jiný typ zařízení podporující pouze anténu externí ?

Odpověď

Ano, zadavatel připouští návrh zařízení s interní anténou a jeho případnou následnou změnu na jiný typ zařízení podporující anténu externí. Uchazeč však musí v nabízeném technickém řešení uvést typ a technický popis zařízení s externí anténou, které bude v případě nutnosti nahrazovat accesspoint s interní anténou. Dále musí být garantováno, že cena základních jednotek accesspointů s interní anténou a accesspointů s externí anténou bude stejná.

V Praze dne 15.2.2010