Dotazy a odpovědi k veřejné zakázce malého rozsahu ze dne 14.11.2011 18:23 hod.
Dodávka bezpečnostního monitorovacího systému SIEM pro ICT v ČSÚ

1). V technickém popisu řešení je požadavek na „Možnost analýzy dat v reálném čase a jejich zobrazení pomocí Event Exploreru" , Event Explorer je pojmenování rozhraní konkrétního produktu konkrétní firmy, tento požadavek by měl být, buď vyřazen, nebo nahrazen obecným pojmem.

Odpověď: Event Explorer je chápán jako prohlížeč událostí, který je součástí SIEM (přívětivé uživatelské prostředí) - lze nahradit výrazem SIEM Explorer.

2). V technickém popisu řešení je požadavek na „Počet současných uživatelů Exploreru" , Explorerem je míněn Internet Explorer nebo Windows Explorer ?

Odpověď: Explorerem je míněn prohlížeč událostí, který je součástí SIEMu.

3). Požadavkem „Možnost připojení externí úložiště" je myšleno jakékoliv úložiště, nebo nějaké konkrétní, které v rámci ČSÚ používáte ?

Odpověď: Pod požadavkem „Možnost připojení externí úložiště" je myšlena možnost připojení na jakékoliv úložiště (např. Oracle DB).

3). Pojmem „Pořízený systém SIEM musí umožnit vysílat výstrahy" výstrahy je myšleno vysílání hlasových výstrah?

Odpověď: Pod požadavkem „Pořízený systém SIEM musí umožnit vysílat výstrahy" je myšleno odesílání výstrahy v emailové formě (nejedná se o hlasovou výstrahu).

4). Formulace „Systém musí být využitelný ke sledování a správě logů síťových zařízení a úložišť, a současně k monitorování hardwaru a používaných aplikací" nám není jasný, síťová zařízení nejsou hardwarem? Jak je to s operačními systémy ty nechcete sledovat ? Používané aplikace je myšleno např. Microsoft Word ?

Odpověď: Pod formulací „Systém musí být využitelný ke sledování a správě logů síťových zařízení a úložišť, a současně k monitorování hardwaru a používaných aplikací" je myšleno např. sledování zařízení Cisco, Oracle DB, vybraných citlivých síťových aplikací používaných v ČSÚ (není myšleno Microsoft Word).

5). Formulace „Systém musí poskytovat inteligentní forenzní nástroj pro odhalování problému s infrastrukturou, pomáhat administrátorům a poskytovat detailní přehled o konkrétním chování konkrétních koncových uživatelů", systém musí poskytovat detailní přehled o konkrétním chování konkrétních koncových uživatelů, konkrétním chováním je myšleno co konkrétně?

Odpověď: Pod formulací „Systém musí poskytovat inteligentní forenzní nástroj pro odhalování problému s infrastrukturou, pomáhat administrátorům a poskytovat detailní přehled o konkrétním chování konkrétních koncových uživatelů....." , je myšleno umožnit bezpečnostním pracovníkům (pracujícím s konsolí SIEMu) reagovat na neoprávněné přístupy uživatelů k příslušným DB nebo aplikacím.

Dotazy a odpovědi k veřejné zakázce malého rozsahu ze dne 15.11.2011 09:06 hod.
Dodávka bezpečnostního monitorovacího systému SIEM pro ICT v ČSÚ

V bodě 13. Výzvy je uvedeno: Při zadávání veřejné zakázky jsou zadavatel i dodavatelé povinni používat výlučně elektronické prostředky dle § 149 zákona. Přitom v bodě 16. Výzvy - Lhůta a místo podání nabídek - uvádíte: Zadavatel umožňuje podání nabídek pouze v listinné formě.
Otázka: Vylučujete tedy podání nabídky elektronickými prostředky - například dodáním nabídky do datové schránky ČSÚ ?

Odpověď: Zadavatel si vyhrazuje při **komunikaci** s dodavateli používat výhradně elektronické prostředky. Dodání **nabídky** prostřednictvím datové schránky nebo mailem se vylučuje.

č.2
V dodatečné informaci k veřejné zakázce SIEM - dne 10.11.2011 je uvedeno, cituji:
"...Součástí dodávky nebudou žádné nosiče a ani software. Tento článek je ve smlouvě irelevantní, můžeme je vynechat?"
V odpovědi na dotaz uvádíte, že článek 9.1 smlouvy lze vynechat. Vynecháním odstavce 9.1 smlouvy, vypadává z předmětu plnění software.
Otázka: Co je tedy předmětem poptávky veřejné zakázky malého rozsahu ? Ve výzvě v bodě 5. Vymezení předmětu veřejné zakázky je uvedeno:
Je požadována dodávka hardwarového zařízení (appliance) SIEM, které obsahuje software jako nedílnou a neoodělitelnou součást tohoto zařízení....

Odpověď: Zadavatel (ČSÚ) zaslal dodatečnou informaci k veřejné zakázce SIEM (dne 10.11.2011) s upřesněním, že součástí dodávky nebudou žádné nosiče se software na nosičích - platí vymezení předmětu veřejné zakázky ve znění: "Je požadována dodávka hardwarového zařízení (appliance) SIEM, které obsahuje software jako nedílnou a neoddělitelnou součástí tohoto zařízení.... ".

Otázka č.3
V technickém popisu předmětu plnění je uvedeno: ... součástí pořízení systému SIEM bude příprava dostatečného počtu výstupů/výkazů systému, zajišťujících shodu s platnými předpisy....
V článku 1. Účel a předmět smlouvy, odstavec 1.2 je uvedeno: ....Součástí předmětu smlouvy je rovněž analýza infrastruktruy ČSÚ k použití SIEM...
Otázka: Pokud ještě Zadavatel neprovedl analýzu infrastruktury ČSÚ k použití SIEM, jaké výstupy/výkazy bude Zadavatel pro zajištění shody s předpisy požadovat ?

Odpověď: Zadavatel (ČSÚ) požaduje dodávku systému SIEM s dostatečným počtem výstupů/výkazů - vstupy a výkazy k zajištění shody s platnými předpisy budou zadavatelem upřesněny před samotnou instalací systému SIEM (na základě dříve získaných zkušeností). Provedení analýzy infrastruktury ČSÚ se požaduje pouze z hlediska způsobu instalace systému do infrastruktury ČSÚ - podrobná analýza infrastruktury ČSÚ k použití SIEM není součástí poptávky.

Otázka č.4:
V návrhu smlouvy v článku 1. Účel a předmět smlouvy, odstavci 1.1. je uvedeno, cituji:
"...který provede v případě zajištěného útoku automatickou karanténní ochranu a zároveň, pokud je útočník detekován ve vlastní síti, přesune ho do karanténní VLAN."
Intrusion Prevention Systems (IPS) - ochrana k detekci a blokování útoků proti síťové infrastruktuře - je požadována v jiné veřejné zakázce malého rozsahu, uvedené pod názvem "Dodávka systému prventivní ochrany IPS pro ICT ČSÚ".
Otázka zní: Je takto specifikovaný předmět plnění veřejné zakázky správný?

Odpověď: Text uvedený v návrhu smlouvy "...který provede v případě zajištěného útoku automatickou karanténní ochranu a zároveň, pokud je útočník detekován ve vlastní síti, přesune ho do karanténní VLAN." je nesprávný (neodpovídá předmětu plnění) - text bude před podpisem smlouvy upraven tak, aby odpovídal předmětu plnění.