MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

MVCRX033ULJN
prvotní identifikátor

Č E S K Á R E P U B L I K A
M I N I S T E R S T V O V N I T R A
Praha 7, Nad Štolou 936/3, IČ: 00007064
zastoupená
JUDr. Petrem Novákem, Ph.D.
ředitelem odboru bezpečnostního výzkumu a vzdělávání
Kontaktní adresa: náměstí Hrdinů 1634/3, 140 21 Praha 4

Č. j. MV-68870-16 /VZ-2016

Praha 19. srpna 2016

Veřejná zakázka – Vybudování a ověřovací provoz Cyber Threat Intelligence – dodatečná informace č. 3

k uveřejnění na profil zadavatele

Na základě ustanovení § 49 odst. zákona č. 137/2006 Sb., o veřejných zakázkách, v platném znění (dále jen „zákon"), Vám zasíláme dodatečnou informaci včetně textu dotazu v rámci veřejné zakázky „Vybudování a ověřovací provoz Cyber Threat Intelligence", která byla vyhlášena ve Věstníku veřejných zakázek pod evidenčním číslem 638646 dne 12. července 2016 a zadavatelem je evidována pod č.j.: MV-68870/VZ-2016.

Zadavatel obdržel tyto dodatečné dotazy:

Dotazy uchazeče"

1. Zadávací dokumentace zmiňuje, že cílem projektu je vytvoření efektivního systému detekce hrozeb. Je požadavkem také implementace bezpečnostního monitorování sítě/sítí nad rámec systému inteligentních analýz a korelačních

schopností? Nebo se jedná pouze o implementaci tohoto systému a všechny požadované datové zdroje jsou již k dispozici?

a. Jaký je případně rozsah požadovaného monitorování sítě/sítí?
b. Existuje SOC (Security Operation Centre) nebo NOC (Network Operation Centre), na kterém by bylo možné stavět?
c. Jaké bezpečnostní zařízení se využívá? Ochrana koncových zařízení, VPN, firewally, aplikační firewally, systémy prevence a detekce průniků, proxy?
d. Existuje interní program nebo proces automatizovaného zjišťování zranitelností?
e. Můžete poskytnout souhrn síťových zařízení (např.: firewally, switche, servery, atd.), které zajišťují bezpečnost na síti/sítích, abychom mohli lépe porozumět rozsahu, v kterém bude monitoring probíhat?
f. Můžete nám prosím poskytnout více detailních informací ohledně rozsahu sítě/sítí (šířku pásma síťového připojení, počet komponentů, počet uživatelů, popis síťové struktury, očekávané množství událostí za sekundu, atd.)?
g. Máte plně funkční SIEM, nebo centralizovaný logovací systém? Pokud tomu tak není, je implementace zařízení systému SIEM vyžadována v rámci tohoto projektu?

2. Můžete stručně popsat, s kým bude v rámci provozu systému potřeba spolupracovat? Kolik to bude přibližně lidí, jaké jsou jejich pozice a dovednosti?
3. Jsou v rámci Ministerstva nějaké funkční a/nebo licencované technologie, které by bylo možné v rámci projektu využít?
4. Existuje v rámci Ministerstva proces řízení incidentů? Můžete ho stručně popsat?
5. Očekáváte od dodavatele zajištění a poskytování IoC (Indicators of Compromise, např. nebezpečné IP adresy, popis vzorů chování atp.)?
6. Jedním z výstupů projektu je „výzkumná zpráva - hodnotící hrozby a rizika kybernetické bezpečnosti v České republice a na základě nich vytvořená doporučení k eliminaci budoucích škod způsobených kybernetickými úkony." Můžete prosím upřesnit očekávání ohledně této zprávy? Jedná se o jednorázové posouzení kybernetických hrozeb v České republice, nebo se jedná o pravidelné provádění reportů s použitím implementovaného systému?
7. Můžete poskytnout více informací ohledně představy využití honeypotů?

8. Nad rámec výše uvedeného, je mezi požadavky také:
    a. Korelace zranitelností poskytovaných třetími stranami nebo jejich nástroji (např. Nessus, AppScan atp.)?
    b. Forenzní analýza zaměřená na sledování stop útočníka krok za krokem?
    c. Koordinace reakce na potenciální komplexní incidenty?

Odpověď zadavatele:

V první řadě se tazatel domnívá, že systém CTI chce budovat resort MV pro své interní účely, čemuž tak není, a proto jsou některé dotazy vzhledem k určení systému „nepřesné“ a lze na ně těžko odpovědět. Nejedná se o standardní veřejnou zakázku, ale o výzkum a vývoj.

1. Projekt je určený pro používání pracovištěm Vládní CERT, což je vládní koordinační bezpečnostní tým. Zdrojem dat pro CTI mohou být otevřené a veřejně dostupné informace, výstupy z různých síťových a monitorovacích zařízení a systémů (např. SIEM) atd. Je na řešiteli/dodavateli, aby navrhl správné fungování tohoto systému včetně možných zdrojů dat. Rovněž by měl navrhnout rozhraní pro přidání dalších, dnes neznámých zdrojů dat a rozhraní pro výstup dat po analýze z CTI do jiného systému. Systém by tedy měl fungovat sám o sobě, ale i jako možný zdroj dat pro případný vyšší navazující systém.
2. V rámci projektu bude nutné spolupracovat s pracovištěm Vládní CERT Národního bezpečnostního úřadu. Bude se jednat o cca 10 osob v různých technických i netechnických funkcích zaměřených na oblast kybernetické bezpečnosti. Počet osob na straně zdrojů dat CTI nejsme schopni posoudit, neboť tyto zdroje by měl v rámci projektu navrhnout dodavatel.
3. Jelikož se nejedná o interní projekt MV, ale je připravován pro pracoviště Vládní CERT NBÚ, které je pouze koordinační a neplní v žádném případě roli správce informačního systému a nestará se o provozní ani bezpečnostní technologie (ani NBÚ), nelze na otázku odpovědět.
4. Jelikož se nejedná o interní projekt MV, ale je připravován pro pracoviště Vládní CERT NBÚ, které je pouze koordinační a neplní v žádném případě roli správce informačního systému a nestará se o provozní ani bezpečnostní technologie a řešení incidentů organizace (ani NBÚ), nelze na otázku odpovědět.
5. V rámci projektu by tyto informace mohly být jak vstup, tak zejména očekáváme, že budou jeden z výstupů pro potřeby Vládního CERT.

6. Výsledek „výzkumná zpráva“ je přesně definován v předpisech týkajících se výzkumu a vývoje[1], neboť se jedná o veřejnou zakázku na službu ve výzkumu a vývoji. Zadavatel požaduje zprávu jako jednorázové zhodnocení projektu výzkumu. Zpráva by měla obsahovat jak zhodnocení a řešení aktuálního stavu, tak i výhled a doporučení do budoucna.
7. Honeypoty a výsledky jejich reportů/analýz mohou být jedním ze zdrojů dat pro projekt CTI.
8. K jednotlivým bodům:
    a. Ano. Toto může být jeden ze zdrojů projektu CTI.
    b. Předmětem projektu CTI není provádění forenzní analýzy. Výsledky analýz ale mohou být zdrojem dat pro CTI.
    c. Ne. Koordinace reakce na incidenty není předmětem projektu CTI.

za zadavatele
JUDr. Petr Novák, Ph.D.
ředitel odboru bezpečnostního výzkumu
a vzdělávání

[1] **Definice výzkumné zprávy dle Metodiky hodnocení výsledků výzkumných organizací a hodnocení výsledků ukončených programů (platná pro léta 2013 až 2016), schválená usnesením vlády ČR:**
Výsledek „Výzkumná zpráva“ realizoval původní výsledek výzkumu, vývoje a inovací, které byly uskutečněny autorem nebo týmem, jehož byl autor členem. Jedná se o takový výsledek, který byl uplatněn v souladu s § 4 písm. g) nařízení vlády č. 267/2002 Sb., do 31. 12. 2009 a od 1. 1. 2010 o uplatněný výsledek v souladu s § 4 písm. g) Nařízení vlády č. 397/2009 Sb., obsahujícím utajované informace podle zvláštního právního předpisu (např. zákon č. 148/1998 Sb., o ochraně utajovaných skutečností a o změně některých zákonů, ve znění pozdějších předpisů, zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů).