U N I V E R Z I T A P A L A C K É H O V O L O M O U C I
Křížkovského 511/8, 771 47 OLOMOUC

č.j.: 520/PS/OVZ/2018 **dne: 26. 10. 2018**

Věc: Vysvětlení zadávací dokumentace č. 2

K veřejné zakázce v nadlimitním režimu na dodávky s názvem: **„Vybudování primárního systému pro prevenci průniku na bázi heuristiky“**, zadávané v otevřeném řízení, uveřejněné ve Věstníku veřejných zakázek pod evid. č. zakázky: **Z2018-033603**, sděluje zadavatel v souladu s § 98 odst. 3 a § 99 odst. 1 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, v účinném znění (dále jen „Zákon“) následující vysvětlení zadávací dokumentace:

Dotaz č. 1:
V kapitole 2.2.2 , odstavci A) Parametry, bodě 1 zadávací dokumentace je požadován parametr min. 20 SFP+ portů.
Otázka: Zadavatel požaduje min. 20 SFP+ portů, ale zároveň je požadováno pouze 8 SFP+ modulů. Máme to chápat tak, že aktuálně se využije pouze 8 portů a v budoucnu lze tento počet dostupných SFP+ rozšířit na min. 20? Pokud se nyní požadovalo 20 SFP+ portů, ale bylo využito pouze 8 portů, jak vyplývá ze ZD, neekonomicky by tento parametr navyšoval soutěžní cenu.

Odpověď:
Zadavatel trvá v návaznosti na své interní potřeby, na dodání min. 20 SFP+ portů.

Dotaz č. 2:
V kapitole 2.2.2 , odstavci A) Parametry, bodě 3 zadávací dokumentace je požadován parametr „Možnost mitigace útoku (kapacita prevence proti DDoS flood útokům) min. 20Gbps“.
Otázka: Zadavatel požaduje kapacitu ochrany proti DDoS útokům 20Gbps, přičež výkon Firewallu požaduje 8 Gbps a poptávané SFP jsou pouze 10Gb. Rádi bychom věděli, jaká

bude rychlost připojení k internetu a protože nepředpokládáme vyšší než 10Gbps (ze znalosti provozovaného prostředí), v tom případě by pak měla kapacita 10Gbps stačit.

Odpověď:
Nikde není požadován "výkon firewallu 8 Gbps", je požadována dle zadávací dokumentace v bodu 2.2.1 "minimální kapacita legitimního provozu", což je jiná charakteristika, která koreluje s požadovanou kapacitou ochrany proti DDoS. Rychlost připojení k internetu není pro výpočet požadované kapacity plně směrodatná, protože zařízení bude obsluhovat i jiný provoz. Kapacita 10Gbps tedy stačit nebude. Zadavatel trvá na dodržení stanovených podmínek.

Dotaz č. 3:
V kapitole 2.2.2 , odstavci D) Bezpečnost – behaviorální analýza provozu , bodě 1 zadávací dokumentace je požadován parametr „Rozpoznávání a blokování zneužití legálních aplikací (L7 floody)“.
Otázka: Co si pod tímto parametrem máme představit, případně prosíme o vysvětlení na konkrétním příkladu?

Odpověď:
Odpověď: jedná se o útoky směřující na aplikace – např. http floody, útoky na DNS službu, na SIP servery. Příklad 1: útočník generuje z botnetu např. http GET requesty na existující webovou stránku s cílem přetížit webový server. Řešení musí byt schopno rozlišit, kdy se jedná o legitimní provoz a kdy se jedná o L7 flood. Příklad 2: dalším příkladem aplikačního floodu je rekurzivní DNS flood - útočník generuje DNS dotaz na subdoménu (řetězec „subdomény“ je generován náhodně) a DNS server pak se ptá nadřazeného DNS serveru na tyto neexistující subdomény – díky tomu dochází k přetížení DNS serveru.

Dotaz č. 4:
V kapitole 2.2.2 , odstavci D) Bezpečnost – behaviorální analýza provozu , bodě 3 zadávací dokumentace je požadován parametr „Rozpoznávání a blokování neznámých útoků (zero day attacks)“.
Otázka: Na základě čeho chcete rozpoznat Zero Day útoky, které jsou z principu velmi těžce identifikovatelné, a díky požadavku na blokaci (v ZD) bude pravděpodobně docházet k velkému množství False positive, tj. blokování legitimního provozu?

Odpověď:
Obecné jméno nástroje na rozpoznávání těchto typů útoku je obsaženo již v samotném názvu veřejné zakázky. Možnost detekovat zero day útoky souvisí se schopností naučit se legitimní provoz, a to metodami implementovanými stávajícími výrobci bezpečnostních zařízení na bázi behaviorální analýzy, strojového učení, umělé inteligence a dalších. V okamžiku, kdy se zařízení naučí legitimní provoz – je možno s velkou přesností detekovat jakoukoliv odchylku a následně ověřit, zda se jedná o útok nebo ne. Tedy ne každá odchylka je útok, ale je nutno sledovat postup 1) nutnost detekce odchylky, 2) následné vyhodnocení, 3) pak vygenerování dynamické signatury a čištění datového provozu.

Signatura musí být schopna sledovat změny a pokud útočník přidá/změní vektory útoku – signatura se přizpůsobí.

Dotaz č. 5:
5) V kapitole 2.2.2 , odstavci D) Bezpečnost – behaviorální analýza provozu , bodě 5 zadávací dokumentace je požadován parametr „Generování dynamických signatur v reálném čase podle probíhajícího útoku“.
Otázka: Na základě čeho má být rozpoznán útok Zero Day a pro jaké typy signatur to platí (Malware, IPS, Reputace)? Máme za to, že za 18s nelze z principu Zero Day útok detekovat – viz. kapitola 2.2.1.

Odpověď:
Zero Day útok z principu neplatí pro klasické statické signatury uvedené v dotazu, neboť jeho signatury vznikají dynamicky na základě analýzy legitimního provozu, viz odpověď na dotaz č. 4. Na trhu existují zařízení, jejichž výrobci tuto predikci včetně daného časového rozpětí nabízejí.

Dotaz č. 6:
V kapitole 2.2.2 , odstavci E) Zapojení v síti , bodě 3 zadávací dokumentace je požadován parametr „Terminace GRE při nasazení v L3 módu“.
Otázka: Myslí tím zadavatel, že je opravdu třeba terminovat GRE tunel přímo na FW, nebo je třeba pouze provést inspekci GRE tunelu? Rádi bychom také věděli, proč je potřeba ukončovat GRE tunel na firewallu, např. z důvodu jeho nezabezpečení?

Odpověď:
Jedná se o terminaci GRE tunelu. Umožňuje to řešit situaci, kdy se poskytuje požadovaná ochrana i subjektům, které nejsou přímo za poptávaným zařízením. Je aplikováno na stávající GRE tunely.

Vzhledem ke skutečnosti, že se jedná pouze o vysvětlení zadávací dokumentace, nikoliv o změnu, zadavatel nemění lhůtu pro podání nabídek.

S pozdravem

Mgr. Pavel Šohaj
Digitálně podepsal Mgr. Pavel Šohaj
Datum: 2018.10.26 09:16:12 +02'00'

Mgr. Petra Vopálková
kontaktní osoba ve věcech veřejné zakázky