Република Србија
МИНИСТАРСТВО ФИНАНСИЈА
Управа за трезор
Сектор за људске и материјалне ресурсе
Број: 404-00-894-2/2014-001-008
25.08.2014. године
Поп Лукина 7-9
Б е о г р а д

Одговор на питање у вези конкурсне документације за јавну набавку добара – Систем за спречавање упада преко Интернета, за потребе Министарства финансија – Управа за трезор, у отвореном поступку, ОП број 43/2014, по партијама

Свим понуђачима који су
преузели конкурсну документацију

Захтев за додатним информацијама или појашњењима Конкурсне документације - ОП 43/2014 – **Систем за спречавање упада преко Интернета**, за потребе Министарства финансија – Управа за трезор.

Поштовани,
Молимо да одговорите на следећа питања у вези конкурсне документације – ОП број 43/2014 како би могли да понудимо решење које што боље одговара Вашим потребама:

Питање 1.

Која је ваша тренутна расподела и количина саобраћаја (traffic/protocol distribution profile and bandwidth)

- Која је расподела Интернет саобраћаја ?
  - Који је профил долазног саобраћаја ?
    - Профил сервиса и протокола (http,https,smtp,dns,streaming protocols, итд..)
    - Која је стварна количина (throughput) најзаступљенијих сервиса и протокола ?
  - Која је профил одлазног саобраћаја:
    - Колико ће корисника бити иза Система за спречавање упада преко интернета (System for Intrusion Prevention) ?
    - Количина (Bandwith utilization) саобраћаја корисника-средња и вршна вредност?

- Који сервиси праве највећу количину (bandwith) саобраћаја ?
- Која је тренутна искоришћеност Интернет саобраћаја (средња вредност/вршна вредност)?

Одговор 1.

Када је у питању расподела Интернет саобраћаја,сервиси и протоколи које Управа за трезор највише користи су: http, https, smtp, dns, ftp, streaming и читав низ других протокола.

<u>Питање</u> 2.

Тражено је 10Gbps пропусне моћи

Да ли то значи да желите да постигнете 10Gbps пуне инспекције саобраћаја са укљученим свим модулима (укључујући Application Control, DLP и Zero-day protection)?

<u>Одговор</u> 2.

Није тражено 10Gbps пропусне моћи него 10Gbps инспектованог саобраћаја. Такође се нигде у тексту не помиње Zero-day protection.

<u>Питање</u> 3.

DLP protection

Молим да детаљније опишете специфичне захтеве за блокаду потпуно непознатих напада.

<u>Одговор</u> 3.

DLP protection значи да је понуђени уређај у стању да без било каквог додатног хардвера или софтвера блокира одлазни саобраћај који у себи садржи информације које Управа за Трезор одреди као поверљиве.

<u>Питање</u> 4.

Блокада потпуно непознатих напада

Молим да детаљније опишете специфичне захтеве за блокаду потпуно непознатих напада.

<u>Одговор</u> 4.

Није довољно да систем блокира само познате нападе и спречава искоришћење познатих рањивости већ да има уграђене способности да блокира потпуно непознате нападе. Није довољно да решење блокира само на основу patern matching сигнатура, већ треба да има уграђену превентивну интелигенцију која: блокира рањивости за које нису још објављени печеви, блокира мутиране нападе, ради бихевиоралрну анализу напада на WWW а све на основу сопствених истраживања која спроводи произвођач опреме.

<u>Питање</u> 5.

Кашњење (latency)

Молим да дате списак апликација које су осетљиве на кашњење (latency) као и која су максимална кашњења која те апликације дозвољавају

<u>Одговор</u> 5.

Уређај треба да подржи voice и video conferencing.

Комисија за јавну набавку