Műszaki leírás
a „DDoS monitoring szolgáltatás”
tárgyú beszerzési eljáráshoz

Nyertes Ajánlattevő feladata Budapest Főváros Főpolgármesteri Hivatal (Ajánlatkérő) informatikai hálózata felé irányuló adatforgalom monitorozása, illetve az esetleges támadásokkal szembeni védelem biztosítása az alábbiak szerint:

A meglévő és folyamatosan működő internetes kapcsolaton DDoS monitoring szolgáltatás és automatikus vagy manuális Layer 3-as és Layer4-es szintű DDoS védelem biztosítása, oly módon, hogy támadás észlelése esetén a védelem automatikusan bekapcsoljon és korlátlan számú és ideig tartó támadást kivédését tegye lehetővé.

A rendszer automatikus beavatkozás megkezdésének Ajánlatkérő által elfogadott maximum ideje 12 perc (7/24), amelynél kedvezőbb időtartam értékelési szempontként került meghatározásra.

Ajánlattevő vállalja, hogy amennyiben az automatikus szűrés nem kapcsol be, vagy nem megfelelő mértékben szűri ki a támadó forgalmat, Ajánlattevő munkatársai 30 percen belül megkezdik a manuális beavatkozást és indokolt esetben a kapcsolatfelvételt az Ajánlatkérővel.

A védelem keretén belül a szolgáltatói hálózat határán elhelyezett berendezésnek folyamatosan mintavételeznie, monitoroznia kell az internetforgalmat. A DDoS rendszernek képesnek kell arra lennie, hogy az Ajánlatkérő felé érkező külső forgalmat teljes mértékben megszűrje, és a támadóforgalmat oly módon blokkolja, hogy az Ajánlatkérő felé csak a legitim forgalom haladjon tovább.

Ajánlattevő feladata továbbá, hogy Layer 7-es szintű DDoS védelmet biztosítson az Ajánlatkérő jelzése esetén. Ilyen esetben Ajánlattevőnek 30 percen belül aktiválnia kell a védelmet és a forgalmát a szűrő rendszerbe terelni.

A DDoS szolgáltatás kiterjed:

1. heti automatikus riport készítése, amely a forgalomról, annak DDoS védelméről minimálisan az alábbi elemeket tartalmazza:

- DDoS riasztásokat: mekkora sávszélességgel, milyen csomagszámmal volt aktív védelem.
- Időrendi grafikonon ábrázolva mekkora volt a teljes vonali kihasználtság.
- Időrendi grafikonon ábrázolva mekkora volt alkalmazásonként (TCP, UDP és IP protokollonként) a vonali kihasználtság. A sávszélesség igény alapján a legnagyobb

forgalmú protokollt, legalább 20 elemű táblázatos formában is meg kell jeleníteni a protokoll nevével és az irányfüggő sávszélesség igénnyel.

- Időrendi grafikonon ábrázolva mekkora volt forrás országonként a vonali kihasználtság. A sávszélesség igény alapján a legnagyobb forgalmú országot, legalább 20 elemű táblázatos formában is meg kell jeleníteni az ország nevével és az irány függő sávszélesség igénnyel.
- Időrendi grafikonon ábrázolva mekkora volt az ICMP forgalom vonali kihasználtsága. A sávszélesség igény alapján a legnagyobb forgalmú ICMP típust legalább 20 elemű táblázatos formában is meg kell jeleníteni az ICMP típus nevével és az irány függő sávszélesség igénnyel.
- Időrendi grafikonon ábrázolva, mekkora volt csomagméretek szerint a forgalom vonali kihasználtsága. A sávszélesség igény alapján a legnagyobb forgalmú csomagméretet legalább 20 elemű táblázatos formában is meg kell jeleníteni a csomagmérettel és az irány függő sávszélesség igénnyel.

2. Támadás esetén az automatikus védelem bekapcsolásának biztosítása, amelyhez szükséges rendszer működőképességéről Ajánlattevő köteles rendszeresen megbizonyosodni és azt folyamatosan üzemkész állapotban tartani. Bármely okból automatikusan el nem hárítható támadás esetén Ajánlattevő köteles a probléma megoldásához szükséges megfelelő tudású és létszámú szakembert biztosítani. Továbbá köteles Ajánlatkérőt a megtett intézkedésekről, az esetleges károkról és az azok elhárítása érdekében tett intézkedésekről a lehető leggyorsabb módon tájékoztatni.