Dotaz:

V příloze zadávací dokumentace č. 1 Specifikace díla máme nejasnost v těchto požadavcích:
„P. 102 Minimální požadavky na EmailSecurity řešení:
1. Řešení musí být výkonově dimenzováno minimálně na 1000 uživatelů a licencováno na 1500 chráněných stanic (využíváno celkem 600 uživateli)…“
a
„P.109 Minimální požadavky na websecurity řešení:
1. Řešení musí být výkonově dimenzováno minimálně na 1000 uživatelů a licencováno na 150 chráněných stanic (využíváno celkem 600 uživateli)…“

Domníváme se správně, že u požadavku P.102 došlo k překlepu, jelikož počet 1500 chráněných stanic nedává smysl v kontextu počtu uživatelů (1000) a relevantní počet požadovaných chráněných stanic je 150 stejně jako v požadavku P.109?

Odpověď:

Požadavek P.102 je v uvedeném parametru definován chybně, správná hodnota je 150. Nová znění požadavku je následující:

P.102	Minimální požadavky na EmailSecurity řešení: 1. Řešení musí být výkonově dimenzováno minimálně na 1000 uživatelů a licencováno na 150 chráněných stanic (využíváno celkem 600 uživateli) 2. nabízené zařízení je možné provozovat v clusteru v režimu loadbalancing, 3. Reputační filtrování na základě zdrojových IP adres odesílatele a reputační způsob blokování spamu na úrovni TCP spojení 4. Možnost nastavení anti-spam akce pro pozitivní nebo podezřelý spam: Doručit, zahodit, karanténa, doručit jako přílohu, přesměrovat 5. Per-user anti-spam karanténa s ověřováním pomocí LDAP 6. Definice whitelist a blacklist pro každého uživatele v karanténě 7. Periodické zasílání notifikací o novém spamu v karanténě pro každého uživatele 8. Možnosti uživatele pro práci se spamem v karanténě: Smazat, doručit, přidat do whitelistu 9. Možnost označit/klasifikovat email jako spam přímo z emailového klienta 10. Detekce a klasifikace marketingových emailů, které nejsou spam 11. Podpora pro současné kontroly více antivirovými engines přímo na zařízení včetně detekce viru uvnitř víceúrovňového archivu 12. Možnost opravy zavirovaných příloh nebo jejich zahození 13. Automatická aktualizace všech antimalware signatur v intervalu 5 minut či méně 14. Per-user nebo per-group nastavení pro Anti-spam a Anti-virus akce pro příjemce či odesílatele 15. Možnost vytváření sofistikovaných filtrů na emailovou komunikaci s možností filtrace na obsah hlaviček, těla i příloh emailu 16. kontrola příchozí i odchozí poštovní komunikace na jednom zařízení zároveň, 17. Filtrování obsahu a ochrana proti úniku dat a. Podpora váhových slovníků b. Podpora pro mezinárodní a multibyte umístění (nejlépe podpora UTF8) c. "Pattern matching" uvnitř vícevrstvých archivů

	d. Plná podpora regulárních výrazů pro "pattern matching" e. Plnohodnotný a pravdivý filetype matching (ne na základě MIME type / filename) f. Detekce chráněných archivů g. Možnost omezit maximální velikost přílohy nebo celého emailu h. Filtrování na základě výsledku DKIM/SPF ověření i. LDAP integrace pro filtrování obsahu j. Per-user a per-group nastavení pro podmiňovací a nápravné akce pro příjemce či odesílatele k. Možnost nápravné akce: Karanténa, upozornění, zahodit email, zahodit přílohu, nahradit přílohu, přesměrovat, kopírovat 18. Modifikace obsahu a zabezpečení dat a. Per-user a per-group nastavení pro modifikaci obsahu a dat pro příjemce či odesílatele b. Podmíněné přidání hlavičky do emailu, možnost přidat tzv. "footer" c. Možnost odstranění hyperlinku URL z textu emailu 19. Funkce SMTP – omezení protokolu např. na a. Omezení maximálního počtu současných spojení per odesílatele b. Omezení maximálního počtu zpráv per spojení c. Omezení maximálního počtu příjemců v emailu d. Omezení maximálního počtu příjemců za hodinu 20. Administrace a management a. HTTPS Management console b. Ověřování a autorizace administrátorů pomocí lokálních účtů a pomocí RADIUS c. Napojení do centrálního dohledu pomocí SNMP d. Podpora centrálního logování pomocí SYSLOG

Změna nemění okruh možných dodavatelů a nedochází tedy k prodloužení termínu podání nabídek.