Zbog promjena koje će naknadno biti javno objavljene objavljujemo odgovore isključivo za Grupu 2, odnosno odgovore koji se odnose na sustav za zaštitu elektroničke pošte.

1.	**U dokumentu Prilog 7. Osnovni zahtjevi za Grupu 2 Ev. broj: 38-21-VV-OP stoji prema rednom broju:** **6. Sustav omogućuje analizu datoteka u izoliranom okruženju (eng. sandboxing) od minimalno 1.000 jedinstvenih datoteka u satu.** Predlažemo naručitelju da omogući iskazivanje kapaciteta analize datoteka u izoliranom okruženju po danu zato što ne iskazuju svi proizvođači vrijednosti po satu. U dokumentu tehnička specifikacija G2 je navedena mogućnost iskazivanja kapaciteta po danu („Sustav analize u izoliranom okruženju mora omogućiti analizu 1.000 jedinstvenih privitka tj datoteka u satu u vršnom opterećenju a 11.000 u danu.“) no isto nije navedeno u dokumentu „Prilog 7. Osnovni zahtjevi za Grupu 2“ Obzirom se u školama osim Windows OS koriste i Linux i MacOS računala za koja se razvijaju zasebne ugroze, predlažemo naručitelju da uvede zahtjev za analizu privitaka elektroničke pošte u Linux i MacOS izoliranom okruženju (sandboxu) čime će sustav omogućiti zaštitu ne samo Windows OS klijenata već i MacOS i Linux klijenata. Obzirom je Sandbox sustav temeljna funkcionalnost traženog sustava predlažemo da naručitelj uvede dodatni kriterij kojim Sandbox sustav mora imati funkcionalnost ručnog unosa datoteka ili sumnjivih URL-ova za skeniranje od strane Sandbox sustava zato što neke sumnjive datoteke odnosno URL poveznice ne moraju biti izravno isporučene e-mail sustavom (npr. prilog e-mailu je komprimirana datoteka zaštićena lozinkom). **25. Uređaj treba moći propusti transparentno sve što prelazi tražene kapacitete inspekcije bez odbacivanja prometa do maksimalne tražene mrežne propusnosti.** Molimo naručitelja da razjasni pitanje, želi li naručitelj promet preko traženog kapaciteta prihvatiti bez inspekcije čime bi se dovela u pitanje svrha ovakvog sustava? Stoga predlažemo naručitelju da navedeni zahtjev preformulira u: Uređaj treba moći propustiti u integriranu karantenu sve poruke elektroničke pošte preko traženog kapaciteta analize datoteka u izoliranom okruženju (eng. sandboxing) do traženog kapaciteta obrade poruka elektroničke pošte u danu, a bez odbacivanja prometa.
Odgovor: 6. Kapacitet analize je izražen i u danu i u satu i trebaju biti oba uvjeta zadovoljena. Isti opis navedenog zahtjeva naručitelj će staviti i u odgovarajući prilog tj. „Prilog 7. Osnovni zahtjevi za Grupu 2“ . Predložene funkcionalnosti ručnog unosa datoteka i URL-a te analize u različitim OS-ovima nisu nužne i mogu biti ograničavajuće stoga ih naručitelj ne prihvaća. 25. Cilj ovog zahtijeva je da promet ne bude „tiho“ odbačen nego da se osigura isporuka do primatelja bilo povratnom porukom prema pošiljatelju koji bi ponovno pokušao poslati ili sa odgođenom inspekcijom. Naručitelj će preformulirati zahtjev na sljedeći način:	

Hrvatska akademska i istraživačka mreža – CARNET
Josipa Marohnića 5, HR - 10000 Zagreb · tel: +385 1 6661 616 · fax: +385 1 6661 615 · mail: ured@carnet.hr · www.CARNET.hr

„Uređaj ne smije odbaciti elektroničku poštu što prelazi tražene kapacitete tj mora napraviti inspekciju sa odgodom ili poslati odgovarajuću povratnu informaciju pošiljatelju u slučaju da nije isporučena.„

2.	**U dokumentu Prilog 9. Dodatni zahtjevi za Grupu 2 ev.broj: 38-21-VV-OP stoji prema rednom broju:** **1. Analiza datoteka u izoliranom okruženju (eng. sandboxing) je dio samog sustava tj na lokaciji sustava (eng. on-premise).** Kako bi sandbox sustav imao nužno potrebne funkcionalnosti zaštite od zlonamjernih datoteka u izoliranom okruženju predlažemo naručitelju uvođenje dodatnog zahtjeva kojim bi sustav analize datoteka u izoliranom okruženju, tzv. Sandbox sustav, mora imati funkcionalnost kontrole i prilagodbe sandbox okruženja kako bi ono bilo relevantno za korisnike u hrvatskim školama. Odnosno u izoliranom okruženju mora se moći definirati verzija, jezik i jezik tipkovnice operativnog sustava, odnosno odabir hrvatskog jezika kao jezika sandbox izoliranog okruženja (obzirom dobar dio ugroza cilja određenu verziju operativnog sustava i jezik), verzije instaliranog Internet preglednika, verzije Microsoft Office paketa i odabir aplikacija koje će biti instalirane u sandbox izoliranom okruženju. Bez mogućnosti ovakve prilagodbe sandbox okruženja ono neće biti relevantno za računala korisnika u hrvatskim školama pa neće biti ostvarena svrha napredne zaštite u izoliranom okruženju. Obzirom su datoteke zaštićene lozinkom često korištene u komunikaciji elektronskom poštom upravo radi zaobilaženja sandbox sustava, predlažemo naručitelju da uvede dodatni zahtjev da ponuđeni sustav mora imati funkcionalnost unosa često korištenih lozinki koje sustav automatski koristi za otvaranje kriptiranih datoteka pri skeniranju. Predlažemo naručitelju da uvede dodatni zahtjev kojim sandbox sustav mora imati uključenu funkcionalnost kojom je moguće aktivirati skeniranje datoteka neuobičajenih ekstenzija a koje su često korištene u maliciozne svrhe, npr.: *.tnef, *winmail.dat, *.win.dat...
Odgovor: Naručitelj ne prihvaća prijedlog gospodarskog subjekta. Dodatne predložene funkcionalnosti nisu neophodne te mogu ograničiti tržišno natjecanje.	

3.	**U dokumentu Prilog 5. Tehnička specifikacija_G2 ev.broj:38-21-VV-OP naveden je zahtjev:** „Maksimalan broj sandučića iznosi 520.000.“ dok je u dokumentu Prilog 7. Osnovni zahtjevi za Grupu 2 Ev. broj: 38-21-VV-OP navedeno „Sustav mora održavati minimalno 520.000 korisničkih računa (sandučića elek. pošte).“ Kako bi zahtjevi bili jednoznačno i jasno definirani predlažemo naručitelju da definira minimalni broj korisničkih računa (sandučića elektronske pošte) za koje **mora biti isporučen sustav, odnosno mora biti isporučena licenca(e) sustava za minimalno navedeni broj korisničkih računa.** Naime, korištenjem formulacije „mora podržavati“

Hrvatska akademska i istraživačka mreža – CARNET
Josipa Marohnića 5, HR - 10000 Zagreb · tel: +385 1 6661 616 · fax: +385 1 6661 615 · mail: ured@carnet.hr · www.CARNET.hr

	može se dovesti zainteresirane ponuditelje u zabludu da je potrebno isporučiti sustav koji podržava navedeni broj sandučića no ne moraju biti isporučene licence za traženi broj sandučića (korisničkih računa). Predlažemo da naručitelj definira zahtjev: „Sustav mora biti isporučen s kapacitetom i svim potrebnim softverskim licencama za minimalno 520.000 korisničkih računa (sandučića elek. pošte).“
Odgovor: U dokumentu Prilog 5. Tehnička specifikacija u poglavlju 7 u četvrtom pasusu stoji da sve navedene i tražene funkcionalnosti u ovom dokumentu i pripadajućim dokumentima sustava za zaštitu, moraju biti isporučene sa svim potrebnim i pripadajućim komponentama te licencama tako da su opisane, navedene i tražene funkcionalnosti ostvarive u trenutku isporuke opreme bez dodatnih troškova za Naručitelja. Također u dokumentu Prilog 7. Osnovni zahtjevi za Grupu 2 stavci 24 stoji Sustav mora imati licence za sve gore navedene funkcionalnosti. Kako je na dva mjesta navedeno da su licence potrebne naručitelj ne prihvaća prijedlog o navođenju licenci, no prihvaća prijedlog u ujednačavanju izričaja i izmijenit će tehničku specifikaciju te maknuti riječ maksimalan.	

4.	**U dokumentu Prilog 5. Tehnička specifikacija_G2 ev.broj:38-21-VV-OP, str. 9 naveden je zahtjev:** Protokoli za upravljanje i nadzor Svi elementi u sustavu moraju podržavati slijedeće upravljačko nadzorne protokole: • SNMPv2, SNMPv3, • SSHv2, • Syslog, • NTP, • AAA putem RADIUS protokola Sustavi za zaštitu prometa elektroničke pošte su specijalizirani sustavi zatvorenog tipa kojima se pristupa kroz web upravljačko sučelje putem HTTP/HTTPS protokola. Pristup internim dijelovima sustava nije predviđen niti omogućen putem SSH protokola. Stoga predlažemo naručitelju da iz popisa protokola za upravljanje i nadzor ukloni zahtjev za podrškom upravljanjem putem SSHv2 protokola a predvidi i omogući mogućnost pristupa HTTP/HTTPS protokolom. Predlažemo naručitelju da za potrebe autentikacije/autorizacije/accountinga (AAA) na sučelje za upravljanje i nadzor dopusti korištenje RADIUS, LDAP ili SAMLv2 protokola.

Hrvatska akademska i istraživačka mreža – CARNET
Josipa Marohnića 5, HR - 10000 Zagreb · tel: +385 1 6661 616 · fax: +385 1 6661 615 · mail: ured@carnet.hr · www.CARNET.hr

Odgovor: Naručitelj u svojoj infrastrukturi i nadzoru infrastrukture koristi sve navedene protokole te su isti nužni za integraciju u postojeću infrastrukturu. Upravljačko sučelje je definirano pod rednim brojem 21 gdje se traži grafičko sučelje (GUI) koje može biti i preko http/https protokola. Ostali protokoli naručitelju nisu nužni.

5.	**Prilog 7. Osnovni zahtjevi za Grupu 2** Tehnička karakteristika pod rednim brojem 14. • mogućnost jednostavnog otpuštanja poruka elektroničke pošte iz karantene od strane administratora i primatelja poruke elektroničke pošte *Pitanje:* Vodeći sustavi zaštite elektroničke pošte, implementiraju više tipova karantena ovisno o stupnju sigurnosne ugroze koju elektronička poruka u sebi sadrži. Primjer su SPAM karantena i Virusna karantena. Mogućnost otpuštanja poruka elektroničke pošte iz karantene od strane primatelja moguće je kod SPAM karantene, dok se kod pojave virusa u elektroničkoj poruci ne dopušta krajnjem korisniku pristup malicioznom sadržaju i mogućnost jednostavnog otpuštanja iz karantene. Po najboljoj praksi pristup elektroničkim porukama s malicioznim sadržajem mora biti omogućen isključivo administratorima sustava. Elektroničke poruke koje se nalaze u drugim karantenama u sebi sadržavaju kritične zlonamjerne poveznice, datoteke i slično, te običan korisnik sustava takvim elektroničkim porukama ne smije imati pristup. Molimo da se tehnička karakteristika pod rednim brojem 14 izmjeni na: • mogućnost jednostavnog otpuštanja poruka elektroničke pošte iz SPAM karantene od strane administratora i primatelja poruke elektroničke pošte • mogućnost jednostavnog otpuštanja poruka elektroničke pošte iz ostalih karantena od strane administratora
Odgovor: Naručitelj prihvaća prijedlog gospodarskog subjekta.	

6.	**Prilog 7. Osnovni zahtjevi za Grupu 2** Tehnička karakteristika pod rednim brojem 16. • Kreiranje vlastitih crnih lista i lista izuzimanja („black and white lists“): - mogućnost kreiranja listi prema odredišnoj adresi, - mogućnost kreiranja listi prema izvorišnoj adresi, - mogućnost kreiranja listi prema naslovu poruke, - mogućnost kreiranja listi prema ključnim riječima *Pitanje:* Vjerodostojnost i provjera pristigle pošte od strane krajnjeg korisnika uvelike se fokusira na prepoznavanje pošiljateljeve mail adrese ili domene. Prilikom provjere pošte krajnji korisnici prepoznaju ili ne prepoznaju pošiljatelja te pošte, te na osnovu toga mogu definirati da li im je pošiljatelj poznat/legitiman ili ne, te odlučuju da li ga staviti na crnu listu ili istu izuzimanja. Ove odluke stavljanja poznatih ili nepoznatih pošiljatelja na liste mora se odnositi isključivo na poruke koje su označene kao potencijalni SPAM i stavljene su u SPAM karantenu. Ostavljanje

Hrvatska akademska i istraživačka mreža – CARNET
Josipa Marohnića 5, HR - 10000 Zagreb · tel: +385 1 6661 616 · fax: +385 1 6661 615 · mail: ured@carnet.hr · www.CARNET.hr

	krajnjem korisniku na volju da kreira vlastite crne liste ili liste izuzimanja za kritične karantene poput Virus karantene dovodi do velikih sigurnosnih propusta i ugroze sustava. Kreiranje listi izuzimanja prema naslovu poruke ili ključnim riječima ne smije biti omogućeno u sustavu za zaštitu elektroničke pošte. Izuzimanje poruka putem ovog načina dobio bi prioritet nad drugim puno važnijim sigurnosnim provjerama poput analiza priloženih datoteka, analiza pošiljatelja i sadržaja poruka, analiza poveznica unutar poruka. Ovakav način implementacije listi izuzimanja doveo bi do velike sigurnosne ugroze cijelog Naručiteljevog sustava te nikako ne smije biti omogućen. Također kreiranje crnih listi putem ostalih parametara mora biti isključivo omogućeno administratorima sustava, a nikako krajnjim korisnicima, kako bi se spriječila sigurnosna ugroza kompletnog Naručiteljevog sustava. Molimo da se tehnička karakteristika pod rednim brojem 14 izmjeni na: • Kreiranje vlastitih crnih lista i lista izuzimanja („black and white lists“) za SPAM karantenu: - mogućnost kreiranja vlastitih listi dodavanjem pošiljatelja za poruke detektirane kao SPAM - mogućnost kreiranja vlastitih listi dodavanjem pošiljateljeve domene na listu za poruke detektirane kao SPAM - mogućnost kreiranja crnih listi pregledom ključnih riječi unutar poruke definiranih od strane administratora - mogućnost kreiranja crnih listi pregledom ključnih riječi unutar naslova poruke definiranih od strane administratora
Odgovor: Ponuditelj djelomično prihvaća prijedlog i definira zahtjev na sljedeći način. Sustav mora podržavati kreiranje vlastitih crnih lista i lista izuzimanja („black and white lists“) za SPAM karantenu: - kreiranje listi prema izvorišnoj adresi, - kreiranje listi prema izvorišnoj domeni, - kreiranje crnih lista prema ključnim riječima u naslovu poruke definiranih od strane administratora, - kreiranje crnih lista prema ključnim riječima unutar poruke definiranih od strane administratora	

7.	**Prilog 7. Osnovni zahtjevi za Grupu 2** Tehnička karakteristika pod rednim brojem 21. Upravljanje: - ugrađena podrška za pristup i administraciju uređaja putem grafičkog sučelja za kontrolu uređaja (GUI), - mogućnost konfiguracije uređaja direktnim spajanjem putem CLI/komandne linije, - mogućnost redovnog centraliziranog ažuriranja softvera i sigurnosnih definicija, - ugrađena mogućnost upravljanja, izvoza i uvoza prijašnjih konfiguracija. *Pitanje:* S obzirom da proizvođači pristupaju različito zadatku ažuriranja softvare-a, backupa konfiguracija i ažuriranje sigurnosnih definicija, od kojih niti jedan način ne ugrožava

Hrvatska akademska i istraživačka mreža – CARNET
Josipa Marohnića 5, HR - 10000 Zagreb · tel: +385 1 6661 616 · fax: +385 1 6661 615 · mail: ured@carnet.hr · www.CARNET.hr

	funkcioniranje sustava za zaštitu prometa elektroničke pošte, predlažemo da se tehnička karakteristika pod rednim brojem 21 izmjeni na: Upravljanje: - ugrađena podrška za pristup i administraciju uređaja putem grafičkog sučelja za kontrolu uređaja (GUI), - mogućnost konfiguracije uređaja direktnim spajanjem putem CLI/komandne linije - mogućnost redovitog ažuriranja sigurnosnih definicija - mogućnost spremanja i dohvaćanja prijašnjih konfiguracija sustava sa udaljenih lokacija ili direktno sa sustava
Odgovor: Naručitelj prihvaća prijedlog gospodarskog subjekta.	

8.	**Prilog 7. Osnovni zahtjevi za Grupu 2** Tehnička karakteristika pod rednim brojem 26. • Uređaj treba moći propusti transparentno sve što prelazi tražene kapacitete inspekcije bez odbacivanja prometa do maksimalne tražene mrežne propusnosti. *Pitanje:* Tražena funkcionalnost sustava za zaštitu elektroničke pošte pozicionira sustav da bude iznimno podložan DDoS napadima i napadima velikom količinom prometa elektroničke pošte, onemogućavajući njegovu primarnu funkciju obavljanja sigurnosne provjere prometa elektroničke pošte. Ovom funkcionalnošću sustav Naručitelja se dovodi u izravnu sigurnosnu prijetnju i ranjivost, te tražena tehnička karakteristika nikako ne smije biti implementirana. Povećanje potrošnje kapaciteta inspekcije sustava za zaštitu prometa elektroničke pošte ne rješava se na način da sustav počne propuštati dio ili svu elektroničku poštu bez analize nego sustav mora imati mogućnost horizontalnog skaliranja i širenja kapaciteta dodavanjem novih poslužiteljskih komponenti bez dodatnog licenciranja. Ovim načinom skaliranja i proširivanja sustava osiguravamo da Naručiteljev sustav elektroničke pošte u svakom trenutku ima dovoljno kapaciteta da sigurnosno analizira promet elektroničke pošte, čineći Naručiteljev sustav u svakom trenutku sigurnim od prijetnji. Iz gore navedenih razloga molimo da se tehnička karakteristika pod rednim brojem 26. izmjeni na: • Podrška za horizontalnim skaliranjem sustava unutar postojećeg licenciranja. Ukoliko se javi potreba za dodatnim resursima obrade prometa, zbog povećanog obujma elektroničke pošte, sustav mora omogućiti proširenje kapaciteta dodavanjem novih poslužiteljskih komponenti bez dodatnog licenciranja.
Odgovor: Cilj ovog zahtijeva je da promet ne bude „tiho“ odbačen nego da se osigura isporuka do primatelja bilo povratnom porukom prema pošiljatelju bilo odgođenom inspekcijom. Naručitelj će preformulirati zahtjev u : • „Uređaj ne smije odbaciti elektroničku poštu što prelazi tražene kapacitete tj mora napraviti inspekciju sa odgodom ili poslati odgovarajuću povratnu informaciju pošiljatelju u slučaju da nije isporučena." „	

Hrvatska akademska i istraživačka mreža – CARNET
Josipa Marohnića 5, HR - 10000 Zagreb · tel: +385 1 6661 616 · fax: +385 1 6661 615 · mail: ured@carnet.hr · www.CARNET.hr

Također naručitelj djelomično prihvaća prijedlog te dodaje sljedeće: • Sustav mora podržavati horizontalno skaliranje sustava unutar postojećeg licenciranja i traženih kapaciteta. Ukoliko se javi potreba za dodatnim resursima obrade prometa koji je obuhvaćen licencama i koji je kapacitetima unutar zahtijevanih kapaciteta, sustav mora omogućiti proširenje kapaciteta dodavanjem novih komponenti bez dodatnog licenciranja i troška za naručitelja.

9.	**Predlažemo funkcionalnosti za Grupu 2:** **Predlažemo funkcionalnost:** Detekcija novonastalih kampanja – sustav mora omogućiti zaštitu od potencijalnih novonastalih (eng. *„Outbreak“*) kampanja koje sadrže maliciozne URL-ove, maliciozni sadržaj, maliciozne privitke, te za koje još nisu definirani sigurnosni potpisi i pravila. **Obrazloženje:** Sustav mora imati mogućnost brzo prepoznati novonastale masovne kampanje koje se pojavljuju na globalnom nivou, za koje još uvijek ne postoje sigurnosni potpisi i pravila, te se prilagoditi istima i kreirati dinamička pravila koja će štiti Naručitelja od ovog tipa prijetnji. Kako bi smanjio stopu lažno pozitivnih detekcija, sustav mora imati mogućnost postojeće poruke koji su detektirane kao novonastala masovna kampanja, spremiti u posebnu karantenu, kako bi omogućio porukama koje su inicijalno detektirane kao članice novonastale masovne kampanje budu još jednom dodatno pregledane prije odbacivanja.
Odgovor: Naručitelj ne prihvaća prijedlog gospodarskog subjekta. Dodatne predložene funkcionalnosti nisu neophodne.	

10.	**Predlažemo funkcionalnosti za Grupu 2:** **Predlažemo funkcionalnost:** Podrška za DNS-based Authentication of Named Entities (DANE) **Obrazloženje:** Sustav mora imati mogućnost spriječiti sve češće vrste napada poput DNS *cache poisoning* i MITM (Engl. MITM – *Man in the middle*) unutar svijeta elektroničke pošte, kako bi osigurao sigurnu komunikaciju s provjerenom destinacijom te onemogućio napadačima da presretnu komunikaciju elektroničke pošte, ne izmjene tok komunikacije ili dobiju pristup informacijama unutar elektroničke pošte.
Odgovor: Naručitelj prihvaća prijedlog.	

11.	**Predlažemo funkcionalnosti za Grupu 2:** **Predlažemo funkcionalnost:** Podrška za naprednu analizu pošiljatelja, koja se bazira na analizi ne samo reputacije IP adrese, reputacije domene s koje pošiljatelj šalje nego dodatnom analizom atributa poput starosti domene s koje pošiljatelj šalje elektroničku poštu. **Obrazloženje:** Kako bi sustav imao puno veću detekciju neželjenih pošiljatelja i SPAM poruka, moramo uzeti u obzir naprednije oblike detekcije dolazećih konekcija koje uključuju ne samo standardne detekcije bazirane na reputacijama nego ulaze dublje u arhitekturu pošiljatelja te

Hrvatska akademska i istraživačka mreža – CARNET
Josipa Marohnića 5, HR - 10000 Zagreb · tel: +385 1 6661 616 · fax: +385 1 6661 615 · mail: ured@carnet.hr · www.CARNET.hr

	analiziraju npr. atribute poput starosti domene. Starost domene je bitan faktor SPAM poruka i neželjenih pošiljatelja koji u slučaju potrebe slanja kampanje kreiraju novu ispravnu arhitekturu koja je sposobna zaobići standardne provjere sigurnosnog sustava za zaštitu elektroničke pošte poput SPF, IP address reputacije i slično. Upravo u ovom slučaju dodatna provjera starosti domene može utjecati na sprječavanje potencijalnog SPAM prometa i omogućiti sustav robusnijim na detekciju SPAM elektroničkih poruka.
Odgovor: Naručitelj prihvaća prijedlog te je isti uvrstio dodavši sljedeću alineju u točku 10: Sustav mora podržavati detekciju i blokiranje poruka elektroničke pošte prema: - …. - Reputaciji IP adrese i domene pošiljatelja te dodatnom analizom atributima poput starosti domene	

12.	**Predlažemo funkcionalnosti za Grupu 2:** **Predlažemo funkcionalnost:** Dokumentacija za ugrađenu API funkcionalnost mora biti javno objavljena, a sam API mora biti besplatan svima za korištenje. **Obrazloženje:** Otvoreni API (često ga zovemo i javni API) je javno dostupno programsko sučelje koje omogućuje pristup inače zatvorenim sustavima. API opisuje način na koji vanjska aplikacija može komunicirati s sustavom. (https://en.wikipedia.org/wiki/Open_API) Korištenje javno dostupne i javno dokumentirane API infrastrukture omogućuje da vanjske aplikacije mogu koristiti podatke skupljene unutar mrežnih sustava škola za unaprjeđenje vlastitog rada. Također javno otvoreni API omogućuje razvojno istraživačke projekte unutar školskog sustava kojima za cilj može biti razvoj vanjskih aplikacija koje će se oslanjati na informacije koje mogu crpiti iz mreže kao što su sustavi za lokaciju u realnom vremenu ili pak statistički modeli ponašanja mreže u svakodnevnom radu. Stoga je od iznimne važnosti da API infrastruktura bude javno dostupna, besplatna za korištenje i javno dokumentirana kako bi poticali mlade generacija na promišljanje kako da se njihovi projekti oslanjaju. Nadalje javno dostupna API infrastruktura u pravilu je stabilnija u smislu da je proizvođač osnovnog sustava izložen širokom krugu razvojnih inženjera i njihovih aplikacija pa se puno rjeđe dešavaju situacije da proizvođač na svoju ruku radi drastične izmjene postojeće API infrastrukture te uzrokuje prestanak rada aplikacija koje se oslanjaju na API pozive. Javno dostupna API infrastruktura potiče inovativnost – dobar primjer su API infrastrukture najinovativnijih tehnoloških tvrtki kao što su Twiter API, Facebook API ili na primjer Google maps API. Stvoreni su s mišlju da razvojni inženjeri širom svijeta mogu razviti aplikacije koje se oslanjaju na njih.
Odgovor: Naručitelj ne prihvaća prijedlog gospodarskog subjekta. Dodatne predložene funkcionalnosti nisu neophodne i mogu utjecati na tržišno natjecanje.	

Hrvatska akademska i istraživačka mreža – CARNET
Josipa Marohnića 5, HR - 10000 Zagreb · tel: +385 1 6661 616 · fax: +385 1 6661 615 · mail: ured@carnet.hr · www.CARNET.hr

13.	**Predlažemo funkcionalnosti za Grupu 2:** **Predlažemo funkcionalnost:** Podrška za prikaz sadržaja određenih tipova malicioznih dokumenata (.ppt, .pptx, .xml, .pdf, .doc, .docx, .dot, dotx) na siguran način **Obrazloženje:** U slučaju da sustav detektira dokument malicioznog tipa, mora imati mogućnost sigurnog prikaza sadržaja tog dokumenta prema primatelju bez ugrožavanja sustava Naručitelja. Ova funkcionalnost omogućila bi primatelju uvid u sadržaj dokumenta iako bi on inicijalno bio odbačen ili stavljen u karantenu. Primjer ove funkcionalnosti je da primljeni MS Word ili sličan dokument s skrivenim malicioznim kodom sustav može isprintati u PDF i time omogućiti primatelju uvid u sadržaj bez izlaganja Naručiteljevog sustava malicioznom sadržaju. Primatelj mora imati opciju zatražiti originalan dokument. Ovim putem uvelike se utječe na smanjivanje broja *false positive*-a.
Odgovor: Naručitelj ne prihvaća prijedlog gospodarskog subjekta. Dodatne predložene funkcionalnosti nisu neophodne.	

14.	**Predlažemo funkcionalnosti za Grupu 2:** **Predlažemo funkcionalnost:** Retroaktivno djelovanje – Kontinuirana analiza datoteka i automatsko povlačenje elektroničkih poruka iz sandučića korisnika u cijelom ili dijelu sustava elektroničke pošte - Ako sustav naknadno sazna da je propustio poruku s privitkom za koju naknadno utvrdi da je maliciozna, automatsko povlači elektroničku poruku iz korisnikovog sandučića. **Obrazloženje:** S obzirom na kritičnost incidenta propuštanja navedene vrste poruke sa malicioznim privitcima, savjetuje se da se ovakvi incidenti ne ostavljaju krajnjim korisnicima da ih samostalno uklanjaju nego da ih sustav automatski ukloni/preusmjeri iz korisnikovog sandučića kako bi se uvelike smanjila mogućnost kompromitacije i ovisnost sigurnosti sustava o radnjama krajnjeg korisnika. Tražena funkcionalnost je iznimno bitna i važna te doprinosi povećanoj sigurnosti sustava, posebno kod pojave novih nepoznatih virusa, što i zna biti najčešći slučaj kod prometa elektroničke pošte.
Odgovor: Naručitelj ne prihvaća prijedlog gospodarskog subjekta. Dodatne predložene funkcionalnosti nisu primjenjive na svu naručiteljevu arhitekturu.	

15.	**Predlažemo funkcionalnosti za Grupu 2:** **Predlažemo funkcionalnost:** Podrška za horizontalnim skaliranjem sustava unutar postojećeg licenciranja. Ukoliko se javi potreba za dodatnim resursima obrade prometa, zbog povećanog obujma elektroničke pošte, sustav mora omogućiti proširenje kapaciteta dodavanjem novih poslužiteljskih komponenti bez dodatnog licenciranja **Obrazloženje:** Preko 90% ukupno pristiglih elektroničkih poruka sustavi za zaštitu odbiju odmah prilikom pokušaja uspostave SMTP konekcije, analizirajući IP adresu pošiljatelja, te minimalno trošeći resurse sustava za zaštitu elektroničke pošte. Upravo ovakav način analize i filtriranja pristigle pošte čine sustave za zaštitu su

Hrvatska akademska i istraživačka mreža – CARNET
Josipa Marohnića 5, HR - 10000 Zagreb · tel: +385 1 6661 616 · fax: +385 1 6661 615 · mail: ured@carnet.hr · www.CARNET.hr

	otporne na DDoS napade i napade velikom količinom elektroničke pošte, jer se svaka pristigla poruka ne mora prihvatiti i slati na sljedeće nivo-e zaštite na analizu. Preduvjet za ovakav način rada sustava je da sustav za zaštitu elektroničkih poruka bude prvi koji prihvaća SMTP konekciju pošiljatelja. Traženi način implementacije sustava za zaštitu analize elektroničke pošte od strane Naručitelja onemogućava prihvat inicijalne pošiljateljeve SMTP konekcije i zahtjeva da se svaka pristigla poruka prihvaća, te analizira na višim razinama kako bi se utvrdila njena legitimnost. Bez osnovnog filtriranja IP adrese pošiljatelja u SMTP konekciji sustav će trošiti iznimne resurse kako bi obradio svaku pristiglu poruku što može dovoditi do brzog trošenja resursa sustava za zaštitu elektroničke pošte, te pozicioniranja sustava da bude podložan DDoS napadima, onemogućavajući njegovo funkcioniranje. Također obzirom na veličinu Naručiteljevog sustava elektroničke pošte te zbog toga i potencijalni rast količine generiranih poruka kroz budućnost, sustav mora pružati mogućnost horizontalnog skaliranja i širenja kapaciteta dodavanjem novih poslužiteljskih komponenti bez dodatnog licenciranja, kako bi u svakom trenutku imao dovoljno resursa za obradu prometa elektroničke pošte.
Odgovor: Naručitelj djelomično prihvaća prijedlog, tj. prihvaća ga u sljedećoj formulaciji: Sustav mora podržavati horizontalno skaliranje sustava unutar postojećeg licenciranja i traženih kapaciteta. Ukoliko se javi potreba za dodatnim resursima obrade prometa koji je obuhvaćen licencama i koji je kapacitetima unutar zahtijevanih kapaciteta, sustav mora omogućiti proširenje kapaciteta dodavanjem novih komponenti bez dodatnog licenciranja i troška za naručitelja.	

16.	**Predlažemo funkcionalnosti za Grupu 2:** **Predlažemo funkcionalnost:** Centralizirana upravljačka komponenta – Sigurnosni sustav za zaštitu elektroničke pošte treba sadržavati centraliziranu upravljačku komponentu koja omogućava sljedeće funkcionalnosti: a) Prikaz zapisa (eng. *log*) toka elektroničke pošte sa svih uređaja za zaštitu elektroničke pošte na jednoj centraliziranoj konzoli b) Konsolidacija izvještaja i podataka sa svih komponenti za zaštitu elektroničke pošte na jednom mjestu kako bi se dobio jedinstven prikaz pravog stanja prometa elektroničke pošte Naručiteljevog sustava (top pošiljatelji, top primatelji, top destinacije, ukupan broj odbačenih poruka, top razlog odbačenih poruka - antivirus, antispam, …) **Obrazloženje:** Sustavi koji se sastoje od više komponenti za obradu prometa u velikoj većini slučajeva implementiraju i centraliziranu komponentu koja olakšava upravljanje, praćenje obrade, nadzor i izvještavanje stanja sustava i prometa koji prolazi kroz njega. Izvještavanje sustava mora biti centralizirano na jednom mjestu

Hrvatska akademska i istraživačka mreža – CARNET
Josipa Marohnića 5, HR - 10000 Zagreb · tel: +385 1 6661 616 · fax: +385 1 6661 615 · mail: ured@carnet.hr · www.CARNET.hr

	kako bi se dobila kompletna statistička slika prikaza prometa koji prolazi kroz sustav za zaštitu elektroničke pošte, a ne kroz svaku pojedinu komponentu zasebno. Također praćenje određene poruke koja prolazi kroz sustav iznimno je bitno, pogotovo prilikom pojave poteškoća kod dostavljanja te poruke u sandučić korisnika. Prilikom analize i praćenja kretanja pošte kroz sustav za zaštitu elektroničke pošte, poruka može proći kroz bilo koju komponentu koja se nalazi u sustavu za zaštitu elektroničke pošte. Naručitelj mora imati opciju pregleda kretanja pošte putem jedne konzole, koja konsolidira informacije sa svih pojedinih komponenti sustava, a ne pregledavajući logove svake komponente zasebno.
Odgovor: Naručitelj djelomično prihvaća prijedlog, tj. prihvaća prijedlog pod točkom a) na izmijenjeni način koji je naveden u nastavku. Izvještaji su definirani i traženi pod točkom 23. u osnovnim zahtjevima. - Sigurnosni sustav za zaštitu elektroničke pošte treba sadržavati centraliziranu upravljačku komponentu koja omogućava prikaz zapisa (eng. log) toka elektroničke pošte sa svih uređaja za zaštitu elektroničke pošte na jednoj centraliziranoj konzoli.	

17.	**Predlažemo funkcionalnosti za Grupu 2:** **Predlažemo funkcionalnost:** Podrška za kreiranje visoko dostupnog sustava kombinacijom virtualnih i fizičkih uredjaja za zaštitu elektroničke pošte **Obrazloženje:** Obzirom na traženi način implementacije koji onemogućava filtriranje elektroničke pošte odmah na razini SMTP konekcije (reputacija IP adrese pošiljatelja), te uzimajući u obzir veliki broja poštanskih sandučića, te sve veći trend korištenja elektroničke pošte kao službeno sredstvo komunikacije, sustav mora biti spreman preuzeti puno veći broj elektroničke pošte na obradu nego u trenutno navedenim u zahtjevima. Povećan volumen prometa elektroničke pošte, da li pristigao putem distributivnog napada ili kroz legitimnu komunikaciju uzrokovat će probleme sustavu za zaštitu elektroničke pošte, te istrošiti njegove resurse - razlog tome je što se svaka poruka mora prihvatiti i proslijediti na više nivoe zaštite i analize, kako bi se utvrdila njena legitimnost. Naručitelj mora imati opciju proširiti inicijalne fizičke kapacitete sustava za zaštitu elektroničke pošte dodavanjem virtualnih komponenti unutar postojeće licence. Kombinacijom fizičkih i virtualnih komponenti Naručitelj se osigurava da se sustav može proširivati po potrebi, efikasno i brzo kako bi adresirao povećan promet elektroničke pošte za trenutne i/ili buduće potrebe, te bio otporan na razne napade poput DDoS-a.
Odgovor: Naručitelj ne prihvaća prijedlog gospodarskog subjekta. Predložena funkcionalnost može ograničiti tržišno natjecanje.	

18.	**Predlažemo funkcionalnosti za Grupu 2:** **Predlažemo funkcionalnost:** Sustav za zaštitu elektroničke pošte omogućava:

Hrvatska akademska i istraživačka mreža – CARNET
Josipa Marohnića 5, HR - 10000 Zagreb · tel: +385 1 6661 616 · fax: +385 1 6661 615 · mail: ured@carnet.hr · www.CARNET.hr

	a) Podrška za grafički prikaz detektiranog incidenta, uključujući tko je sve unutar sustava primio malicioznu elektroničku poruku, tko su bili pošiljatelji maliciozne poruke, s kojih odredišta i kakve reputacije su ta odredišta s kojih su poslane maliciozne elektroničke poruke, te da li su te maliciozne elektroničke poruke imale priložene maliciozne datoteke b) Podrška za integraciju putem API-a i konsolidaciju sigurnosnih podataka dobivenih sa različitih drugih sigurnosnih uredjaja, radi potrebe istraživanja opsega prijetnje c) Podrška za automatsku obnovu/osvježavanje Bijele Liste/Crne Liste prilikom detekcije prijetnje **Obrazloženje:** Obzirom da govorimo o sigurnosnim rješenjima, osim detektiranja i blokiranja prijetnji, jedna od glavnih odlika kvalitetno implementiranog sigurnosnog rješenja mora biti: • Brzi pregled proširenja incidenta i zahvaćenih korisnika sustava prilikom incidenta, kako bi se što prije sanirala načinjena šteta unutar Naručiteljevog sustava • Sposobnost sustava da se automatski prilagodi novonastaloj situaciji kako bi što prije spriječilo daljnju štetu i širenje incidenta • Komunikacija i dijeljenje informacija putem API-a sa drugim sigurnosnim rješenjima kako bi se dobila šira slika i razumijevanje detektirane prijetnje i incidenta Uzimajući u obzir veličinu Naručiteljevog sustava elektroničke pošte, prilikom nastalog incidenta bez gore navedenih značajki, administratori sustava izgubiti će puno vremena istraživajući incident, te time izravno ugroziti ostatak sustava. Istraživanje incidenta mora biti jednostavno, vremenski kratko i efikasno. Sustav sa gore navedenim značajkama upravo to i omogućava. Sustav mora omogućavati grafički prikaz toka incidenta, te prikazati proširenje incidenta unutar sustava, kako bi administratori sustava pravovremeno znali poduzeti ključne korake u suzbijanju potencijalne štete nastale prilikom incidenta, saniranju štete i zatvaranje sigurnosnih rupa unutar sustava putem kojih se proboj i dogodio. U slučaju pojave incidenta unutar sustava, Naručitelj mora moći programirati uključene komponente sustava za automatsko djelovanje za suzbijanje prijetnje kako se ista ne bi ponovila.
Odgovor: Naručitelj ne prihvaća prijedlog gospodarskog subjekta. Dodatne predložene funkcionalnosti nisu neophodne.	

19.	**Predlažemo funkcionalnosti za Grupu 2:** **Predlažemo funkcionalnost:** Podrška za upravljanje prometom elektroničke pošte i nakon isteka licence **Obrazloženje:** Implementacija sustava za zaštitu elektroničke pošte postavljen je na način da sav ili veći dio prometa elektroničke pošte prolazi kroz direktno kroz njega. Kako bi izbjegao se scenarij prekida osnovne dostave i upravljanja elektroničkom poštom do krajnjeg korisnika, sustav mora imati mogućnost osnovnog upravljanja (eng. *routing*) elektroničkom poštom i nakon isteka licenci. Ovom funkcionalnošću Naručitelj se osigurava da i nakon isteka licenci može zadržati postojeću arhitekturu i koristiti

Hrvatska akademska i istraživačka mreža – CARNET
Josipa Marohnića 5, HR - 10000 Zagreb · tel: +385 1 6661 616 · fax: +385 1 6661 615 · mail: ured@carnet.hr · www.CARNET.hr

	sustav za zaštitu elektroničke pošte kao osnovni MTA, te upravljati prometom elektroničke pošte.
Odgovor: Naručitelj ne prihvaća prijedlog gospodarskog subjekta. Dodatne predložene funkcionalnosti nisu neophodne u planiranoj arhitekturi.	

20.	**Predlažemo funkcionalnosti za Grupu 2:** **Predlažemo funkcionalnost:** Podrška za prihvaćanje sigurnosnih definicija od 3rd party nezavisnih izvora putem STIX-TAXII protokola **Obrazloženje:** Zbog sve veće količine i različitih vrsta napada koje primjećujemo unazad zadnjih par godina, unutar sigurnosnog svijeta gotovo nemoguće da jedan proizvođač može spriječiti sve napade. Upravo iz toga razloga javila se potreba za promjenom načina obrade prometa kod sigurnosnih sustava. Kako bi se spriječilo uspješno prodiranje novih prijetnji u sustav – dijeljenje sigurnosnih informacija između proizvođača postala je jedna od glavnih značajki kvalitetno implementiranog sigurnosnog rješenja. Dodatno ako uzmemo u obzir da je elektronička pošta i dalje glavni vektor napada na sustave, unutar koje se vrše različite vrste napada poput dostavljanja malicioznih datoteka, URL poveznica, *phising* poruka za krađu identiteta i slično, iznimno je bitno da sustav za zaštitu elektroničke pošte ima mogućnost korištenja sigurnosnih definicija razvijenih od strane različitih proizvođača kako bi sigurnosni sustav kombinacijom sigurnosnih definicija razvijenih od strane drugih proizvođača i svojih vlastitih sigurnosnih definicija bio što robusniji i otporniji na prijetnje. Analizom dostupnih rješenja na tržištu zaključili smo da vodeći sustavi zaštite elektroničke pošte prihvaćaju sigurnosne definicije putem STIX-TAXII protokola kako bi postigli efikasno i automatizirano prikupljanje sigurnosnih definicija.
Odgovor: Naručitelj ne prihvaća prijedlog gospodarskog subjekta. Dodatne predložene funkcionalnosti nisu neophodne u planiranoj arhitekturi.	

21.	**Predlažemo funkcionalnosti za Grupu 2:** **Predlažemo funkcionalnost:** Podrška za minimalno dvije istovremene AntiVirus zaštite prilikom obrade priloženih datoteka unutar elektroničke pošte **Obrazloženje:** Unutar sigurnosnog svijeta gotovo nemoguće da jedan proizvođač može spriječiti sve napade. Upravo iz toga razloga javila se potreba za promjenom načina obrade prometa kod sigurnosnih sustava. Kako bi se spriječilo uspješno prodiranje novih prijetnji u sustav – dijeljenje sigurnosnih informacija između proizvođača postala je jedna od glavnih značajki kvalitetno implementiranog sigurnosnog rješenja. Visok postotak uspješno izvedenih napada virusom, odvijaju se upravo kroz dostavljanje zaražene datoteke putem elektroničke pošte do krajnjeg korisnika. Kako bi sustav za zaštitu elektroničke pošte učinili robusnijim i otpornijim na učestale

Hrvatska akademska i istraživačka mreža – CARNET
Josipa Marohnića 5, HR - 10000 Zagreb · tel: +385 1 6661 616 · fax: +385 1 6661 615 · mail: ured@carnet.hr · www.CARNET.hr

	napade, sustav mora imati mogućnost obrade priloženih datoteka unutar elektroničke pošte istovremeno sa vlastitim sigurnosnim definicijama i barem jednim dodatnim sigurnosnim definicijama razvijenim od strane drugog proizvođača.
Odgovor: Naručitelj ne prihvaća prijedlog gospodarskog subjekta. Dodatne predložene funkcionalnosti nisu neophodne i mogu ograničiti tržišno natjecanje.	

22.	Grupa-2-G2-Prilog_7_OSNOVNI_ZAHTJEVI_G2 – prijedlog da se zahtjev pod rednim brojem 2 dozvoli mogućnost nuđenja i rješenja s dovoljnim brojem 1G sučelja (da 10G sučelja ne bude ograničavajući faktor), a koji će omogućiti zadovoljavanje svih ostalih zahtijevanih tehničkih karakteristika osobito vezanih za zahtijevane kapacitete, performanse i propusnosti.
Odgovor: Naručitelj pretpostavlja da se pitanje odnosi na točku 5 u kojoj se traže mrežna sučelja. Naručitelj ne prihvaća prijedlog gospodarskog subjekta.	

23.	Grupa-2-G2-Prilog_9_DODATNI_ZAHTJEVI_G2 – prijedlog da se dodatni zahtjev pod rednim brojem 2 ne boduje kao jedna stavka od 3 boda, već kao 3 stavke od 1 boda. Na taj način bi bila pravednija razdioba bodova po zahtijevanim funkcionalnostima.
Odgovor: Naručitelj ne prihvaća prijedlog gospodarskog subjekta. Nužne su sve nabrojane stavke pa ih se boduje zajedno.	

24.	Predlažemo da se ujednače troškovniče opcije na način da se zahtjeva jednak broj godina za licence i jamstvo, s obzirom da velika većina proizvođača rješenja ne odvaja zasebno jamstvo od licenci, te na taj način je nemoguće ponuditi odvojene stavke jamstva i licenci ukoliko su različita trajanja.
Odgovor: Različit broj godina je bio za potrebe istraživanja. Naručitelj planira staviti isti broj godina za licence i produljeno jamstvo.	

Hrvatska akademska i istraživačka mreža – CARNET
Josipa Marohnića 5, HR - 10000 Zagreb · tel: +385 1 6661 616 · fax: +385 1 6661 615 · mail: ured@carnet.hr · www.CARNET.hr