Приложение № 1

ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ

за „Доставка на „on-premises“ софтуер за специализирано виртуално устройство за защита на имейл-трафика и филтриране на съдържанието“

Софтуерът да отговаря на следните минимални изисквания:

Възможности	
Операционна система	Стабилна и защитена операционна система на базата на Linux.
Файлова система	Файлова система, създадена и оптимизирана за работа с опашки от съобщения.
Mail Transport Agents (MTA)	Sendmail
Едновременни SMTP връзки	10 000 с динамична опашка за всеки защитен домейн.
Антивирусен модул	С минимум три сканиращи устройства, защита срещу новопоявили се заплахи (Zero Hour Module) и сканиране на прикачени файлове.
Поддържани имейл клиенти	Microsoft Outlook 2010, 2013, 2016; Windows Live Mail (Windows 7); Mozilla Thunderbird 31; Lotus Notes 8.0, 8.5.
Поддържани уебмейл клиенти	Microsoft Outlook Web Access 2010, 2013, 2016; Lotus iNotes 7.0.2, 8.5; Messenger Express; Gmail, Hotmail, and Yahoo Mail;
Импортиране на потребители	Интеграция с: LDAP; Microsoft Active Directory; Microsoft Exchange Server 2013, 2016; Импортиране от файл.
Защита срещу Denial of Service	- Контрол на SMTP сесията и ограничаване на потребителския трафик (до ниво получател); - Оценка на репутацията в зависимост от IP адреса / областта, домейн и е-мейл.
Защита срещу изтичане на данни	Възможност за предоставяне на интегрирана Data Loss Prevention (DLP) функционалност и криптиране на поверителната информация, така че тя да не напуска физически рамките на организацията.
Защита срещу Directory Harvest Attack	- Идентификация на невалидни получатели; - „SMTP conversational bounce” за невалидни получатели; - Защита от „Non-Delivery Report Attack”; - Контрол на максималния брой „bounces” за час поради невалидни е-мейл получатели, на база на оценка на репутацията на изпращача.
Контрол на входящия и изходящия трафик	Сканиране и контрол на входящия и изходящия трафик от едно устройство.
Поддържане на множество от домейни	Множество домейни за един IP адрес или множество домейни с различни IP адреси върху единично устройство.
Управление на потребителските политики	- За единичен потребител, на базата на адреса на изпращача, получателя, домейн, или LDAP-група. - Единичен мейл до множество получатели да може да бъде обработван с различни политики; - Възможност за генериране на справка за всички приложено потребителски политики.
Политики за оценка на изпращача	- Черни списъци по IP, домейн и репутация (blacklists); - Бели списъци по IP, домейн и репутация (whitelist); - Използване на допълнителни Real-Time Black List (RBL) списъци; - Проверка на имейлите на изпращача и получателя за присъствие в

	дефинирани бели и черни списъци.
Детайлни мейл политики (Fine granularity)	Политики за изпращача, на базата на: - Максимален брой съобщения на връзка; - Задаване на максимален брой получатели; - Задаване на максимален размер на съобщение; - Задаване на максимален брой конкурентни сесии за IP адрес; - Възможност за настройка на TLS криптиране; - Възможност за настройка на SMTP автентикация.
Филтриране на прикачени файлове	Филтриране на прикачени файлове по: - Тип на файла (file type); - Име на файла (file name); - Разширение на файла (file extension); - MIME type.
Карантина	- Карантина, която се съхранява на самото устройство; - Възможност всеки потребител да получава периодични известия по e-mail относно карантинираните съобщения, адресирани до него и възможност за освобождаване от карантината или докладване за спам или сигурен изпращач (персонални бели и черни списъци).
Контрол на достъпа до карантинната зона	- Контрол на достъпа до област от карантината; - Контрол на потребителско име и парола на карантинните зони, така че различните карантинни зони да бъдат достъпвани само от оторизиран персонал.
Опции за търсене на сканирани съобщения	По получател, изпращач или част от контекста на съобщението.
Генериране на статистики в реално време	Брой на генерираните статистики, но не по-малък от 40.
Доклади	Възможност за web-publishing, изпращане по e-mail или експортиране.
Анти-спам	- Само-обучаваща се технология от трето поколение с анализ на повече от 1.000.000 атрибута; - Защитна стена за имейл трафика; - Анти спам на две нива - превантивно и реактивно на базата на Database Reputation Filters; - Филтриране на базата на репутация (IP на изпращача/домейн); - Технология за засичане в зависимост от контекста на съобщението; - Технология за адаптивно самообучение за точен анализ на съдържанието; - Използване на smart-identifiers за алгоритмични проверки; - Наличие на управляеми речници – предефинирани и обновяеми библиотеки, включително и осъществяване на проверка за спазването на регулаторни изисквания; - Възможност за защита на дигиталните активи чрез функция document fingerprinting (защита от изтичане на данни); - Защита от „zero-day“ атаки; - Проследяване на „zero-day“ фишинг съобщения; - Филтриране на входяща и изходяща поща; - Ефективност от минимум 99,5%.
Превантивна защита от вируси – „Virus Outbreak Filter”	Превантивна защита от вирусни експлозии на базата на ненормално увеличение на е-мейли със специфични прикачени файлове (attachments).
Обновяване	Автоматично обновяване на софтуера и сигнатурите.
Политики	- Минимален брой на предефинираните типове политики – 20; - Възможност за задаване на отделни политики за различни категории, включително и наличие на отделни карантини - Spam,

	Virus, Bulk и др.; - Функция „self-remediation“ на база на репутация; - Грануларни и конфигурируеми политики за фишинг съобщения, включително и наличие на отделна карантина за тях; - Задаване на политики с IP адрес на изпращача; - Задаване на политики с hostname на изпращача; - Задаване на политики с локален IP адрес; -Задаване на политики с Country code; - Задаване на политики по-изпращач или група от изпращачи; - Задаване на политики по-получател или група от получатели; - Възможност за комбиниране на условията за задаване на политики; - Възможност за дефиниране на сканирания трафик - изходящ/входящ, само изходящ или само входящ.
Техническа поддръжка	Техническата поддръжка да се осигурява от сертифициран специалист за работа с предлаганото виртуално устройство с време за реакция при възникнал проблем в рамките на 2ч.
Криптогафски протокол	Вградена TLS поддръжка
Съвместимост	Съвместимост с Microsoft Exchange 2013 и 2016 и всеки тип защитна стена.
Отдалечен достъп	Достъп по HTTPS (web-конзола) и SSH.
Възможност за диагностика	Диагностика от Web-конзола, преглед на лог файлове, експортиране на диагностичен файл.

Съдържание на лицензионния пакет		
	Вид на лицензa	**Брой**
1.	Едногодишен лиценз на база пощенска кутия, включващ техническа поддръжка.	3000

Участникът следва да предостави възможност за инсталиране на софтуера в сградата на ДАЕУ **/”on-premises”/.**