УТВЕРЖДАЮ

Директор

АО «Гидропроект»

_____Паратов Р.А.

ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ
к модернизации системы информационной безопасности

Проектом предусматривается модернизация системы информационной безопасности (далее по тексту – «ИБ») Акционерного общества «ГИДРОПРОЕКТ»:

1) Продление периода гарантийной поддержки и подписок на сервисы информационной безопасности для эксплуатируемых межсетевых экранов следующего поколения;
2) Подписка на сервисы информационной безопасности для обеспечения централизованной защиты конечных устройств от вредоносного программного обеспечения;
3) Создание системы сбора и анализа событий информационной безопасности, поступающих от межсетевых экранов следующего поколения и системы централизованной защиты рабочих станций.

КОМПОНЕНТЫ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Межсетевые экраны следующего поколения

В настоящее время в системе ИБ АО «ГИДРОПРОЕКТ» эксплуатируются следующие межсетевые экраны следующего поколения:

1) Fortinet FortiGate 40F (серийный номер FGT40FTK22049419);
2) Fortinet FortiGate 200E (серийный номер FG200ETK18920416).

Для данных устройств должны быть приобретены:

1) Поддержка программного и аппаратного обеспечения Fortinet FortiCare Premium на 1 год;
2) Подписка на сервисы информационной безопасности Fortinet FortiGuard (Advanced Malware Protection, IPS, URL/DNS/Video Filtering, AntiSpam) 1 год.

Централизованная защита конечных устройств

Комплекс централизованной защиты конечных устройств должен:

- обеспечивать защиту путем установки специализированного программного обеспечения на конечные устройства;
- поддерживать автоматический карантин для конечных устройств без участия оператора;
- поддерживать web-фильтрацию трафика с возможностью ограничения доступа к определённым категориям сайтов;

- обеспечивать защиту конечных устройств от программ-шифровальщиков;
- поддерживать интеграцию с системой двухфакторной аутентификации, в том числе с применением токенов с одноразовыми паролями временного действия;
- поддерживать функциональность сканера уязвимостей с возможность автоматической установки патчей для приложений;
- обладать функционалом межсетевого экрана приложений;
- обеспечивать мониторинг состояния конечных устройств в реальном времени;
- обеспечивать функционал антивируса следующего поколения на базе искусственного интеллекта;
- регулярно получать обновления сигнатур модулей безопасности с сервера производителя;
- поддерживать удалённое развертывание, настройку и централизованное управление из единой консоли (графического интерфейса) администратора;
- иметь встроенный функционал или поддерживать интеграцию с внешними системами для передачи телеметрии, включающей информацию о пользователях, используемой модели операционной системы, используемой версии операционной системы, IP-адреса, MAC-адреса, назначенного профиля;
- иметь возможность интеграции с системой централизованного сбора событий и передачи информации обо всех зарегистрированных клиентах в данную систему;
- при интеграции с системой централизованного сбора событий передавать в нее всю необходимую информацию для построения сводных отчетов по узлам и угрозам, веб-фильтрам, отчет по угрозам по времени, устройствам и/или пользователям, отчет по использованию VPN;
- иметь возможность отправлять подозрительные файлы в песочницу для защиты от угроз нулевого дня;
- иметь возможность контроля подключаемых USB-устройств;
- поддерживать сбор телеметрических данных с конечных устройств, обеспечивать функцию динамической категоризации для интеграции с внешней системой межсетевого экранирования для обеспечения контроля доступа;
- поддерживать возможность передачи информации об учетной записи текущего пользователя Active Directory для реализации прозрачной аутентификации пользователей;
- иметь возможность локальной установки системы централизованного управления на серверное оборудование Заказчика;
- быть масштабируемым методом лицензионного расширения;
- поддерживать в качестве хранилища локальную базу данных Microsoft SQL Server Express, а также базу данных Microsoft SQL Server Enterprise;
- поддерживать управление на основе групп, иметь интеграцию с Microsoft Active Directory для централизованного развертывания клиентов на конечных устройствах, в том числе - с помощью групповых политик.

- поддерживать возможность устанавливать соединения виртуальных частных сетей (VPN) – SSL и IPSec, в том числе с применением двухфакторной аутентификации и сертификатов;
- поддерживать централизованное управление сертификатами;
- обеспечивать просмотр включенных функций, операционной системы, имени узла, IP-адреса и иной системной информации;
- отображать статус клиентского программного обеспечения для каждого устройства;
- поддерживать распространение XML конфигурации;
- обеспечивать возможность отправки односторонних уведомлений группе пользователей по определенному признаку или выбранному пользователю;
- обеспечивать возможность интеграции с решениями контроля привилегированного доступа.

Поддержка операционных систем:

- Microsoft Windows 11/10/8/7;
- Microsoft Windows Server 2012 и более свежие версии;
- Mac OS X 11 и более свежие версии.

Требования к подпискам и технической поддержке:

- Гарантийная поддержка аппаратного обеспечения – не менее 1 года;
- Подписка на сервисы информационной безопасности – не менее 1 год;
- Количество защищаемых конечных устройств - 300.

Система сбора и анализа событий информационной безопасности

В ходе реализации проекта должна быть создана система сбора и анализа событий информационной безопасности, поступающих от различных компонентов системы ИБ (включая межсетевые экраны следующего поколения и систему централизованной защиты конечных устройств).

Система должна обеспечивать централизованное хранение оперативных журналов событий ИБ для целей последующего анализа и аудита в течение срока не менее 3 месяцев. Дополнительно должно быть предусмотрено архивное хранение журналов за период не менее 36 месяцев в виде резервной копии.

Техническое задание составил:

Начальник отдела ИКТ **У.Э. Инагамджанов**