ОТЧЁТ ПО ПРОВЕДЕННОЙ РАБОТЕ АКИМАТА ГОРОДА АЛМАТЫ

Передающая сторона:
ТОО «Inova Tech»
Генеральный директор
Асылбеков С.Ж.

Оглавление

1 ОБЩАЯ ИНФОРМАЦИЯ..... 2
2 АВГУСТ..... 3
3 СЕНТЯБРЬ..... 4
4 ОКТЯБРЬ..... 5
5 НОЯБРЬ..... 7
6 ДЕКАБРЬ..... 8
7 РЕЗУЛЬТАТ..... 9

Общая информация

По результатам 3 квартала Поставщик предоставлял услуги, связанные с проведением анализа технического парка рабочих станций и сетевого оборудования заказчика для установки необходимых компонентов, для пусконаладки систем мониторинга. Также были проделаны работы по монтажу серверного оборудования в инфраструктуре заказчика.

После обследования и отправки отчета о первичном аудите Поставщик приступил к установке и конфигурации ПО для реализации пунктов технической спецификации по обеспечению услуг информационной безопасности. В данный этап также вошло предоставление внутренней документации для Заказчика и проведение обучение для сотрудников Акимата. Начиная с ноября 2024 г. осуществляется мониторинг событий информационной безопасности и оповещения заказчика в соответствие с регламентом взаимодействия между сторонами предоставленным Поставщиком от 7 октября.

Август

1. Формирование и утверждение планов проведения работ.

Со стороны Поставщика были предоставлены План-граф и Диаграмма Ганта с описанием работ, которые были разделены на этапы. С каждой стороны сформировались рабочие группы ответственные за этапы работ. В целях фиксации результатов работ в план-графике были отображены характеристики завершения каждого этапа.

В рамках выполнения пункта 10.8 технической спецификации команда Заказчика совместно с командой Поставщика подготовила презентационный материал с верхнеуровневым описанием проекта в целях осведомленности руководителей подразделений для правильного понимания дальнейших работ со стороны персонала.

2. Получение доступов и запрос необходимой информации для проведения работ.

Со стороны Заказчика были предоставлены доступы на объекты проведения работ с 9 сентября 2024 г. Таже 18 августа 2024 года Заказчик по запросу Поставщика предоставил доступную информацию по наличию оборудования и результаты предыдущих инвентаризаций. Со стороны Поставщика был подготовлен список вопросов по технической части, который в последующем использовали для внутреннего запроса информации среди всех подразделений, в инфраструктуре которых осуществлялась работа.

3. Формирование рабочей группы.

Ответственные лица за проект со стороны Заказчика:

Дюсюков Мейрам - Заместитель руководителя Управления цифровизации города Алматы;

Нургыйсаев Нуржан - и.о. Руководителя отдела информационной безопасности и управления данными;

Дәндібай Аманбол - Главный специалист отдела информационной безопасности и управления данными.

Ответственные лица за проект со стороны Поставщика:
Токарев Кирилл - Проектный менеджер;
Халель Алия - Архитектор MDR;
Жаксыгали Фараби - Архитектор MDR.

Сентябрь

1. Установка и настройка серверов заказчика.

В рамках проекта, после предоставления доступов от 9 сентября рабочая группа Поставщика произвела конфигурацию и установку из доступного серверного оборудования Заказчика в серверной комнате №1, 2 этаж, по адресу площадь Республики 4. На данное оборудование была установлена актуальная ОС и сервер был введен в общую схему подключения, а также настроено VPN соединение. Данное оборудование было предоставлено Заказчиком для размещения на нем системы предотвращения утечек конфиденциальной информации (DLP) и системы обнаружения и реагирования на хакерские атаки и атаки вредоносного программного обеспечения. В момент установки возникли задержки в связи с отсутствием питания в стойках с серверами, однако данных задача решилось путем проведения электричества со стороны Заказчика и предоставлением дополнительных сетевых фильтров со стороны Поставщика.

2. Установка NGFW.

Данный задача была выполнена в рамках пункта 12 технической спецификации к действующему проекту и являлась неотъемлемой частью защиты и фильтрации трафика и соответствия пункта о регуляторных требованиях, указанных в технической спецификации. В период проведение данных работ техническая группа Заказчика пересмотрела и утвердила с Поставщиком несколько вариантов внедрения NGFW в сетевую инфраструктуру заказчика, учитывая все ее особенности и по возможности, не навредив сотрудникам Акимата в период реализации схемы. Конечный вариант внедрения NGFW был отображен в отчете о результатах первичного аудита, принятого Заказчиком 7 октября 2024 г.

3. Инвентаризация рабочих станций.

Начиная с 9 сентября 2024 года Поставщик проводил работы по инвентаризации рабочих станций исходя из пункта 10.5 технической спецификации для реализации отчета о первичном аудите и определению списка устройств подлежащему дальнейшему мониторингу с учетом технических характеристик устанавливаемого для этого программного обеспечения.

В ходе проведения инвентаризации были выявлены следующие факты:

• Зафиксировано 1400 рабочих станций.

• 163 рабочие станции не соответствуют минимальным требованиям для установки ПО (DLP, EDR).

• 1237 рабочих станций соответствуют требованиям для установки ПО (DLP, EDR).

В период выполнения работ наблюдались трудности с отсутствием сотрудников управлений на рабочих местах в связи с отпуском, командировкой или больничным, однако данная задача была решена после официального запроса в каждое управление с целью назначения ответственного лица от каждого подразделения для более оперативной реализации проекта.

4. Инвентаризация сети.

Начиная с 26 сентября осуществлялся этап инвентаризации сети заказчика с перечислением всех сетевых устройств и характеристик пропускной способности каналов. Поставщик предоставил список необходимых вопросов, а Заказчик в свою очередь в соответствие с пунктом 5.9 действующей технической спецификации распределил данный запрос внутри структуры Акимата.

Результат запроса был получен 30 сентября и отображал неполный список управлений. Данная проблема была решена путем обзвона администраторов каждого управления со стоны Поставщика и Заказчика для уточнения необходимых характеристик каналов связи.

По результатам запроса в последующем отчете было отображено 205 единиц сетевого оборудования, 15 серверов и 4 межсетевых экранов, находящихся в инфраструктуре заказчика.

Октябрь

1. Настройка оборудования

В данном этапе Поставщик осуществлял внос оборудования в сопровождении соответствующих актов внесения, которые были одобрены Заказчиком для осуществления услуг в рамках SLA:

1) Коммутатор MicroTik – 2 шт.
2) Next Gen Firewall Check Point 2000 – 2 шт.
3) Next Gen Firewall Check Point 1575 – 11 шт.
4) Оптоволоконный трансивер – 24 шт.

Предоставленное оборудование полностью соответствовало описанию Заказчика, согласно пункту 12 технической спецификации.

Конфигурация оборудования (NGFW и коммутаторов) осуществлялась командой Поставщика и в ходе конфигурации повлияла на финальное видение схемы подключения каналов связи для осуществления фильтрации трафиков. Многие технические моменты необходимо было изменить в связи с несоответствием полученной информации (пропускная способность и информация о статическом IP адресе) в результате запроса от 26 сентября, касательно сетевой инфраструктуры Заказчика. В ходе данного несоответствия наблюдались сбои в работе сети. Решением послужило более тщательный анализ и детальное изучение инфраструктуры

подразделения перед ее подключением с привлечением администраторов, что замедлило ход работы.

В последующем во избежание аварийных ситуаций переключение согласовывалось путем уведомления Заказчика от рабочей группы Поставщика.

2. Настройка DLP

По данному пункту Поставщик установил необходимые элементы системы обнаружения и предотвращения утечек конфиденциальной информации на серверах Заказчика в соответствие с требованиями 1.2.6. После установки системы был разработан список, сверясь с которым происходила оперативная блокировка утечек конфиденциальной информации.

Технические характеристики системы полностью соответствует пункту 4.7.1 требований технической спецификации, работая со всеми перечисленными каналами распространения данных.

3. Настройка PAM

На основании пункта 6 технической спецификации была внедрена система привилегированного доступа в инфраструктуре заказчика, что позволило выделить администраторов систем. Поставщик создал в инфраструктуре заказчика выделенный Бастион безопасности на базе системы Privileged Access Management в соответствии с внутренней нормативной документацией, которая была сформирована у заказчика в ноябре. Задержки в установке были вызваны желанием вендора сопровождать процесс внедрения для корректной работы в инфраструктуре Заказчика и принудительным привлечением специалистов Поставщика получением сертификации по работе.

4. Настройка SIEM системы

Для работы с анализом данных и мониторингом событий информационной безопасности в рамках выполнения пункту 1.2.4. Для настройки системы в соответствие регуляторным требованиями Поставщик разместил виртуальные машины (logstash) для дальнейшей обработки и визуализации информации, поступающей с системы класса EDR.

5. Предоставление обучения

На основании пункта 8 технической спецификации Поставщик предоставил обучение сотрудникам Заказчика в количестве лицензий 1285 шт. в соответствии с количеством сотрудников в акимате, которое предоставил заказчик. Ответственный со стороны Заказчика за обучение путем уведомления был назначен Нургыйсаев Нуржан.

Изначально все заявленные функции платформы корректно работали, однако после проведение встречи с вендором и обработки замечаний, сотрудники приступили к обучению в соответствие с планом представленным Поставщиком.

Ноябрь

1. Разработка внутренней нормативной документации

В соответствие с требованиями 1.2.4 технической спецификации Поставщик предоставил внутренние нормативные документы в количестве 7 штук для Заказчика. Предоставленные правила адаптированы под инфраструктуру Заказчика.

Отдельно был разработал регламент взаимодействия между Поставщиком и Заказчиком. Регламент устанавливает порядок взаимодействия Поставщика и Заказчика по вопросам оказания услуги по обеспечению информационной безопасности и описывает процедуры, связанные с выявлением и реагированием на инциденты информационной безопасности.

Взаимодействие ОЦИБ Поставщика и Заказчика включает в себя регистрацию заявок, организацию процесса восстановления сервиса, взаимное информирование ответственных руководителей компаний о ходе решения вопросов, связанных с восстановлением требуемого качества сервиса.

2. Сканирование уязвимостей и фиксирование защищенности

На основании пункта 13 технической спецификации Поставщик произвел сканирование в соответствие с требованиями Заказчика и предоставил в виде отчета по каждому управлению. Сканирование откладывалось в связи с необъединенной сетевой инфраструктурой, однако со стороны Поставщика было принято решение сканировать каждое управление без привязки к указанному пункту. Рабочая группа проводила анализ каждого сегмента проверяя его по отдельности.

3. Объединение сети в инфраструктуре заказчика

В рамках объединения сети согласно пункту 11 технической спецификации:

- Пункт 11.1 был выполнен со стороны Поставщика путем предоставления отчета по первичному аудиту от 7 октября 2024 года описывающий текущее состояние объектов, который был составлен на основании фактов, предоставленных Заказчиком в отчет на письмо от 26 сентября 2024 года. Все работы по этому направлению выполнены Поставщиком, а именно был проведен анализ сетевой инфраструктуры разработан и утвержден план редизайна сетевой инфраструктуры, описанный в отчете по первичному аудиту от 26 сентября 2024 года;
- Пункт 11.2 был выполнен со стороны Поставщика путем сегментации сети. В рамках данного пункта реализована схема из пункта 11.2 и при этом другие подсети находящиеся по этому адресу не имеют доступа к другим управлениям.

В ходе работ Поставщик неоднократно сталкивался с проблемами перевода управлений в связи с неактуальной информацией, полученной ранее, однако данные задачи решались путем организации работы между Заказчиком, его провайдером и Поставщиком.

4. Установка GRC

В соответствие с требованиями технической спецификации было установлена система управление рисками информационной безопасности. Также со стороны Поставщика была разработана нормативная документация для дальнейшего использования системы Заказчиком. Данная система учитывалась так как являлась одним из критериев для системы межсетевого экранирования.

По результатам внедрения полностью соответствует функционалу.

5. Мониторинг событий и их журналирование событий

Мониторинг событий производится на указанных в отчете о первичном аулите рабочих станциях в связи с требованиями со стороны системы к минимальным требованиям.

После настройки SIEM системы и с учетом формирования регламента взаимодействия между сторонами, начиная с ноября осуществляется журналирование и анализ событий в инфраструктуре Заказчика. В случае возникновения события Поставщик описывал возникающую аномалию, направлял инструкцию по исправлению на почту Заказчика, указанную ранее:

1) a.dandibay@a-a.kz
2) Data@a-a.kz
3) b.kadyrov@a-a.kz

События можно отследить в личном кабинете в соответствие с требованиями в пункте 3 технической спецификации.

Декабрь

1. Установка защиты от таргетированных атак.

Поставщик в рамках пункта 2 технической спецификации предоставил защиту от таргетированных атак в виде внедрения дополнительного оборудования (сервера для Anti-APT) по адресу Республика 4, 2 этаж, 1 серверная. Совместно с верндором Поставщик произвел наладку оборудования и его внедрение в сетевую инфраструктуру Заказчика. Решение от TLab осуществляет поведенческий и статический анализ объектов на предмет вредоносных действий, обнаружение и блокирование угроз ВПО.

В ходе работ были трудности с допуском сотрудников верндора, которые должны были заниматься пусконаладкой серверного оборудования Anti-APT. Данная задача была решена путем сопровождения специалистов представителями Заказчика.

2. Распределение NGFW по районным акиматам и управлениям

Для выполнения данного пункта технической спецификации, начиная с 9 декабря Поставщик распределил оборудование Next Gen Firewall Check Point 1575– 11 шт. и комплектующие для установки по адресам указанным Заказчиком. Данное оборудование осуществляет задачу фильтрации трафика в подразделениях, удаленных от адреса проспект Республика 4.

В ходе работ Поставщик столкнулся с проблемой неактуальности предоставленной информации со стороны Заказчика. Данная задача была решена увеличением рабочей группы и направлением запросов в сторону Заказчика от Поставщика для дальнейшей обработки со стороны провайдера.

3. Распределение Агентов (DLP и ELK) по районным акиматам и управлениям

Для реализации пункта технической спецификации по предотвращению утечек конфиденциальной информации и осуществления мониторинга событий информационной безопасности, сотрудниками Поставщика установлены агенты системы DLP и EDR. Установлено 480 агентов, которые отображают текущую информацию о состоянии инфраструктуры в виде наличия вирусных ПО или подозрительных процессов.

Данная работа была осложнена отсутствием пользователей на рабочих местах в связи с отпуском/больничным/командировкой, однако командой Поставщика данная задача была выполнена дополнительным привлечением специалистов, работой в выходные дни и повторным обходом подразделений для установки агентов.

Результат

По результатам работ Поставщик выполнил:

1. Предоставление план-графика с предположительным временем работы;
2. Актуализацию списка рабочих станций и сетевого оборудования с их перечислением;
3. Визуализацию и утверждение логической схемы инфраструктуры для дальнейшей реализации фильтрации трафика;
4. Предоставление отчета первичного аудита;
5. Установка серверного оборудования в инфраструктуре Заказчика;
6. Установлено и настроено оборудование в серверной комнате Заказчика;
7. Настроены система утечек данных, установлено 480 агентов данной системы;
8. Настроена система мониторинга событий путем установки сбора логов, журналирования и размещением 480 агентов класса EDR на рабочих станциях Заказчика;
9. Предоставлено обучение 1285 сотрудников Заказчика для повышения осведомленности по направлению непрерывности бизнеса и процессов обеспечения ИБ;
10. Установка и конфигурация системы управления рисками информационной безопасности на серверах Заказчика;
11. Установка и конфигурация защиты от таргетированных атак в виде размещения серверного оборудования в инфраструктуре Заказчика;
12. Настройка системы привилегированного доступа в системе Заказчика;
13. Проделаны работы по приведению сетевой инфраструктуры Заказчика к нормативным требованиям, указанным в технической спецификации

14. Распределены и установлены Next Gen Firewall в количестве 11 шт. по предоставленным Заказчиком адресам.
15. Разработаны и предоставлены нормативные документы (включающие 17 тем указанных в технической спецификации) для их дальнейшего внедрения.
16. Настроен мониторинг и журналирование событий в соответствии с регуляторными требованиями, позволяющее обнаруживать и реагировать на события информационной безопасности в инфраструктуре Заказчика.