СТЕК
ИТ ИНТЕГРАТОР

Отчет о результатах экспресс-аудита ИТ-инфраструктуры компании

Данный документ является образцом предоставляемой компанией СТЕК отчетности по результатам проведения комплексного исследования ит-инфраструктуры.

Если у вас возникнут вопросы или потребуются дополнительные пояснения, адресуйте их напрямую эксперту:

+7 965 022 73 40

info@stekspb.ru

Оглавление

Введение

В данном документе отражены результаты обследования информационной инфраструктуры компании "_____", проводившегося в июне 2020 года. Аудит проводился с помощью удаленного подключения. Основной упор был сделан на настройки информационной безопасности операционных систем и серверных приложений. Кроме этого, документ содержит некоторые рекомендации по устранению выявленных недостатков в организации и функционировании обследованной системы.

1. Серверные системы

1.1 Описание серверов, служб и приложений

1.1.1 Описание

Информационная структура компании состоит из 4 физических серверов. Из них 2 Windows server, 1 сборка ip-телефонии Elastix, 1 сборка интернет-шлюза Kerio. Также в серверной группировке присутствует NAS QNAP, выполняющий роль файлового сервера.

Сеть компании построена на пассивных коммутаторах (в основном DLink), все информационные сервисы и рабочие станции находятся в одном адресном пространстве

Основными сервисами для бизнеса являются:

1. Электронная почта – на базе Exchange Server 2013
2. Учетная система 1С.
3. Файловый сервер, находящийся на NAS QNAP
4. IP-телефония

1.1.2 Наименование, ОС, аппаратное обеспечение серверов, распределение служб, ролей и приложений по серверам

Рис.1 Схема сети, предоставленная ИТ-службой “_____ ”

СХЕМА

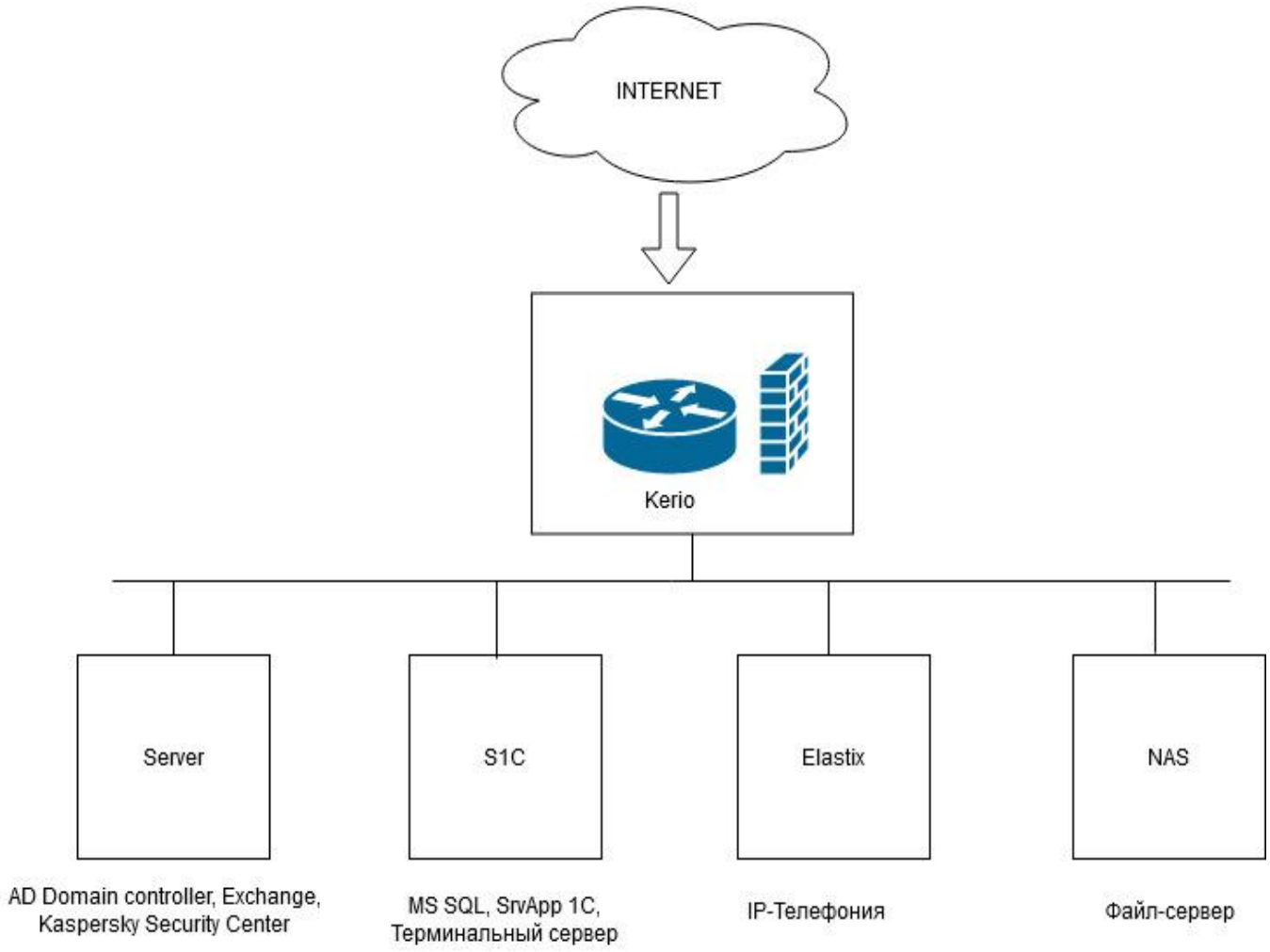

Рис.2 Серверная инфраструктура на данный момент

Табл.1 Серверная инфраструктура ч.1

№	Название	IP адрес	RAID, Модель	CPU, модель	DDR, Гб	HDD, Гб	HDD Free, Гб
1	Server		Нет	Intel Xeon E5-2620v2	DDR3, 16 Гб	1. SSD 180 Гб 2.HDD 1Тб 3.HDD 1Тб	25 Гб 390 Гб 695 Гб
2	S1C		Нет	Intel Core i7-2600	DDR3, 32 Гб	1.SSD 250 Гб 2.SSD 1 Тб 3. HDD 1.5 Тб	125 Гб 755 Гб 530 Гб

Табл.2 Серверная инфраструктура ч.2

№	Название	IP адрес	Физический виртуальный	ОС	Функциональность
1	Server		Физ.	Win 2008 R2 Server Standard	Контроллер домена, Exchange, Kaspersky Security Center
2	S1C		Физ.	Win 2008 Server Standard	СУБД MS SQL, серверное приложение 1С, сервер терминалов
3	Kerio		Физ.	CentOS	Шлюз Интернет, Firewall
4	Elastix		Физ.	CentOS	IP-телефония
5	NAS		Физ.		Файловый сервер

1.1.3 Выявленные проблемы

1. Отсутствие на серверах RAID-контроллеров. При выходе из строя одного жесткого диска весь сервер перестанет функционировать на продолжительное время (замена диска, восстановление информации из резервной копии). При отсутствии резервной копии – безвозвратная потеря бизнес-информации.

2. Неправильное размещение информационных сервисов на серверах. По стандартам безопасности ИТ рекомендуется размещать по одному информационному сервису в операционной системе. В данном случае это не так. И тем более серьезным пробелом в безопасности является совмещение сервера терминального доступа, куда могут зайти все пользователи, с хранением базы данных учетной системы предприятия. Совмещение почтового сервера с контроллером домена тоже очень небезопасное сочетание, так как Exchange может быть атакован через web-интерфейс почтового клиента, а контроллер домена хранит в себе данные об учетных записях и паролях всех пользователей сети предприятия.

3. Отсутствие резервного доменного контроллера. В случае выхода из строя доменного контроллера все пользователи сети предприятия не смогут нормально работать даже на своих рабочих станциях, не говоря уже о серверных приложениях, так как не смогут авторизоваться в операционной системе. Если же доменный контроллер не удастся восстановить в прежнем состоянии, то время восстановления работы может составить несколько дней, так как придется перенастраивать все сервера и рабочие станции.

4. Отсутствие виртуализации. Данная структура сети очень хорошо ложится в концепцию виртуальных серверов. Виртуализация IP-телефонии, шлюза Интернет, доменного контроллера дает возможность на порядок уменьшить время восстановления этих сервисов в случае их серьезно выхода из строя.

2. Базовые службы ИТ-инфраструктуры

2.1 Текущее состояние

2.1.1 Структура службы доступа к каталогам

Структура службы доступа к каталогам организована на базе Microsoft Domain с доменным именем .local. Контроллер домена один, находится на физическом сервере Server, ОС Windows Server2008R2. Доменные политики используются минимально.

2.1.2 Структура службы терминалов

Служба терминалов развернута на сервере S1c, ОС Windows Server 2008. Также на этом сервере находятся СУБД MS SQL и серверное приложение 1С.

2.1.3 Файловые серверы

Основные файловые ресурсы расположены на NAS Qnap. NAS использует доменную авторизацию, используемая файловая система ext4 (linux-based).

2.1.4 Почтовые службы

Почтовая служба развернута на сервере Microsoft Exchange 2013, находящемся на физическом сервере – контроллере домена Server.

2.1.5 Службы управления БД

Базы находятся на физическом сервере S1C на СУБД MS SQL 2008R2. На сервере опубликовано 4 БД, относящихся к 1С. Максимальная из них – 18 Гб данные, 2.8 Гб лог.

2.1.6 Службы управления антивирусом

На предприятии присутствует централизованно управляемый антивирус Касперского, версия – Total Security. Сервер управления расположен на доменном контроллере Server. Компьютеры и серверы не разделены по группам, применяемая политика не кастомизирована, т.е. не настроена на специфику предприятия.

2.1.7 Службы резервного копирования

Резервное копирование на сервере Server производится встроенными средствами на локальный диск.

Резервное копирование баз 1С на сервере S1C происходит через периодическую выгрузку из 1С. В процессе резервного копирования нередко возникают ошибки. Резервное копирование системы производится встроенными средствами ОС. Все резервные копии находятся на локальном диске сервера.

Резервное копирование конфигураций Интернет-шлюза и IP-АТС отсутствует.

Резервное копирование файлов на NAS отсутствует. Есть жесткий диск со старой копией файлов.

2.2 Выявленные проблемы

1. Практически **ОТСУТСТВИЕ РЕЗЕРВНЫХ КОПИЙ БИЗНЕС-ИНФОРМАЦИИ**. Выход из строя любого сервера или атака на него приведет к остановке информационной работы предприятия очень надолго и практически 100% потере информации. При условии отсутствия RAID-контроллеров достаточно будет выхода из строя одного жесткого диска.
2. **Ненастроенные политики антивируса Касперского**. Total Security – очень мощный инструмент обеспечения информационно безопасности предприятия. При его правильной тонкой настройке 80% угроз можно диагностировать и ликвидировать в самом начале атаке. Рекомендуется сделать раздельные политики для серверов, обычных рабочих станций и ноутбуков, выносимых за границы периметра предприятия. Включить политику ограничения разрешенных приложений, ограничить посещение опасных сайтов, не разрешать пользователям отключать антивирус на рабочих станциях – иначе все настройки могут быть бесполезны.
3. **Отсутствие обновлений на ключевых серверных приложениях**. На серверные ОС обновления устанавливаются регулярно, тем не менее на MS SQL и MS Exchange не установлены актуальные SP (сервис-пак) и CU (кумулятивный апдейт).
4. До аудита веб-интерфейс почтового клиента и управления почтовым сервером был опубликован в Интернет без ограничений. В процессе аудита было указано на это нарушение безопасности, и сейчас доступ из Интернет отключен.
5. В сети предприятия присутствует достаточно много устаревших пользовательских операционных систем (Windows XP), устаревшая серверная ОС (Windows Server 2008) и пользовательские приложения (MS Office 2007). По ним прекращена поддержка Microsoft и не выпускаются актуальные обновления безопасности, это значит, что эти программы могут быть потенциально уязвимы.
6. На NAS из-за файловой системы ext4 (linux-based) невозможно гибко выставить разрешения на файлы и каталоги.
7. Настройки для оптимизации СУБД сделаны не оптимально, нужно настроить периодические профилактические работы по индексации всех баз.
8. Некорректно настроена служба RDP, развернуто много лишних компонентов, которые не работают
9. Некорректно настроена служба DNS на доменном контроллере, почтовые клиенты получают адрес сервера с внешним ip-адресом, а не с внутренним.

3. Топология LAN/WAN

3.1 Текущее состояние

В качестве шлюза Интернет и файрвола используется Kerio Control актуальной версии. Коммутация внутри локальной сети осуществляется пассивными устройствами, в основном производства DLink. Активные сетевые устройства не используются. Общая схема на рис.1

3.2 Выявленные проблемы

- Управление сервером Kerio Control было опубликовано по web-протоколу без ограничений в сети Интернет. В процессе аудита было указано на это серьезное нарушение безопасности. Сейчас доступ к управлению Kerio из Интернет отключен.
- В Kerio была включена служба доступа VPN, хотя ею никто не пользуется. Неиспользуемые службы, опубликованные в Интернет лучше отключить (**отключено в процессе аудита**).
- В Kerio не была включена настройка проверки на вирусы текущего почтового трафика (**настроено в процессе аудита**).
- Отсутствие активных сетевых устройств и плоское построение сети без использования VLAN и без разделения на зоны затрудняет диагностику при сбоях внутри локальной сети. Время поиска аварийного сетевого устройства будет сильно увеличено и все это время локальную сеть будет лихорадить.

4. Рекомендации по исправлению проблем

4.1 Рекомендации по реконфигурации серверного оборудования и ИТ-инфраструктуры

- Перенос файлового сервера на доменный контроллер, освобождение NAS.
- Добавление в NAS двух жестких дисков (2 HDD по 6 Тб), настройка NAS
- Настройка резервного копирования бизнес-данных с сервера Server и с сервера S1C на NAS.
- Необходима установка двух RAID-контроллеров (по одному на каждый сервер)
- Добавление в оба сервера жестких дисков для использования в режиме RAID10 (8 SSD дисков по 1 Тб)
- Необходима переустановка операционной системы и внедрение виртуализации Hyper-V на сервере Server

- Рекомендуется переустановка операционной системы на сервере S1C на Windows Server 2008R2 или Windows Server 2012R2
- Необходимо виртуализировать и перенести на виртуальную платформу Server сервер ip-телефонии Elastix
- Необходимо виртуализировать и перенести на виртуальную платформу интернет-шлюз Kerio
- Необходима оптимизация настроек сервера MS SQL. Оптимизация работы с памятью, настройка периодических регламентных заданий по оптимизации БД.
- Необходима настройка сервера Касперского для увеличения безопасности серверов и рабочих станций
- Рекомендуется заменить пассивные сетевые устройства коммутации на активные с функцией защиты от закольцевания сети (протокол STP, RSTP и т.д.) и защиты от broadcasting storm.

4.2 Описание планируемого проекта

По нашему мнению, для того чтобы приблизить ИТ-инфраструктуру к стандартам отрасли не получится по кусочкам сделать настройки на существующих серверах. Необходимо полностью переустановить серверную группировку, внедрить виртуализацию, настроить резервное копирование на выделенный ресурс. Для этого необходимо приобрести серверную платформу, соответствующую требованиям используемых в компании бизнес-приложений. Ориентировочная стоимость такой платформы составляет 250 тыс. руб. Этот сервер будет служить “буфером”, в который будут перемещаться переустановленные ИТ-сервисы.
Также можно оптимизировать существующий сервер SERVER:
- добавить в него оперативной памяти
- установить RAID-контроллер и расширив дисковую систему,
- установить более производительный процессор, совместимый с платформой
ИТ сервисы с сервера Server будут перенесены на новую серверную платформу и переустановлены как виртуальные машины. В процессе этого переноса будет освобожден от файлового хранилища NAS и на него будет настроено резервное копирование бизнес-данных. После освобождения сервер Server будет пересобран и переустановлен, и на него будут перенесены сервисы с сервера S1C. В дальнейшем также будет произведен перенос IP-телефонии и шлюза Интернет на платформу виртуализации – это необходимо для ускорения восстановления этих сервисов при авариях.

Ориентировочный план проекта

1. Установка ОС и платформы виртуализации на новый сервер
2. Миграция сервера Active Directory на новый сервер в виртуальную машину, оптимизация
3. Перенос файлового сервера с NAS на новый сервер Active Directory (простой файлового сервера 3-4 часа)
4. Настройка резервного копирования бизнес-данных на освобожденный NAS
5. Миграция почтового сервера на новый сервер в виртуальную машину, оптимизация
6. Перенос сервера Kaspersky Security Center на новый сервер в виртуальную машину
7. Настройка сервера Kaspersky Security Center для улучшения защиты рабочих станций и серверов
8. Пересборка (установка нового процессора, дисковой подсистемы и т.д.) и переустановка ОС освобожденного сервера Server
9. Миграция терминального сервера в виртуальную машину, оптимизация (простой терминального сервера 3-4 часа)
10. Миграция сервера СУБД и серверного приложения 1С на сервер Server, оптимизация (простой 1С 3-4 часа)
11. Виртуализация сервера IP-телефонии
12. Виртуализация шлюза Интернет
13. Настройка резервного копирования виртуальных машин ip-телефонии и шлюза Интернет

Ориентировочное время выполнения проекта 70-80 рабочих часов

Рис.3 Серверная инфраструктура после выполнения проекта