Аудит рисков ИТ-инфраструктуры

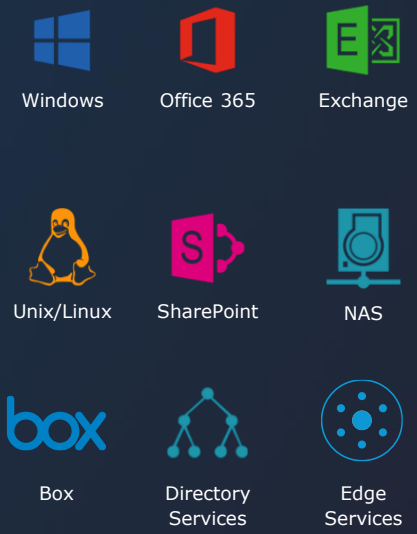
Пример отчёта*

* Данный отчет содержит демонстрационные данные

Содержание

- Избыточные права и разрешения доступа
- Классификация и поиск конфиденциальных документов
- Зоны риска:
  - конфиденциальные данные, доступные всем сотрудникам
  - нестандартная активность пользователей
  - уязвимости и некорректная конфигурация Active Directory
  - другие выявленные риски

> Результаты аудита:
> Развернутые рекомендации и конкретные шаги по устранению выявленных уязвимостей



VARONIS

Анализ рисков на файловых серверах

66 502 975 папок в общем доступе

339 213 456 конфиденциальных документов доступно всем

85 377 723 папок с устаревшими данными

58 419

58 419 папок с некорректными разрешениями

950 534 645 файлов содержит конфиденциальные данные

94 525

94 525 папок с прямыми разрешениями

Анализ рисков на файловых серверах

- Папки с полными правами у не администраторов – это потенциальная угроза:
  - неконтролируемой раздачи прав обычным пользователям
  - лишения доступа других пользователей или служб
  - нарушения структуры прав за счет сброса прав для всех нижерасположенных каталогов

Файловый сервер	Путь доступа	Имя пользователя	Текущие разрешения
FS01	D:\Share\Отдел продаж	Смирнов Н.О.	FMRWXL
FS01	D:\Share\Отел HR\Конфиденциально	HR-Private	FMRWXL
FS01	D:\Share\Бухгалтерия	Пользователи домена	FMRWXL

Анализ рисков на файловых серверах

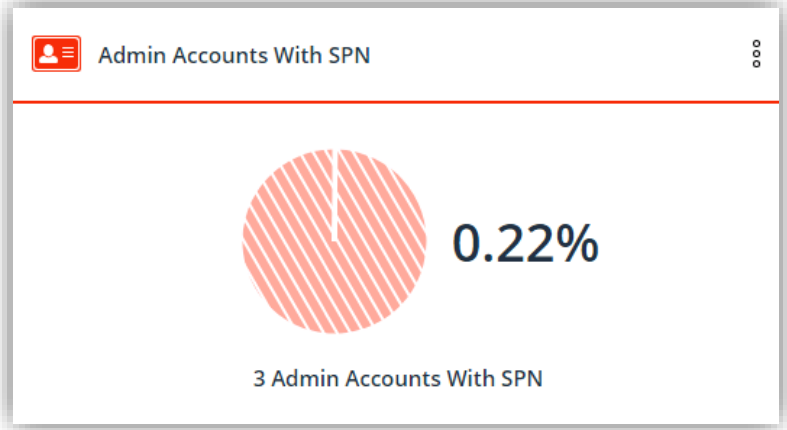
- Папки с доступом для всех пользователей:
  - являются частой причиной утечки данных;
  - способствуют быстрому распространению вирусов-шифровальщиков и нарушению бизнес-процессов
  - Вызывают трудности при прохождении аудита

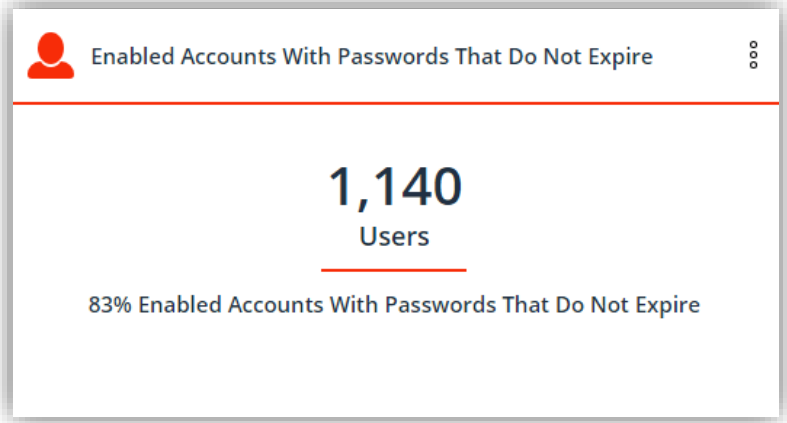
Файловый сервер	Путь доступа	Имя пользователя	Текущие разрешения	Источник прав
FS01	D:\Share\Базы данных\Oracle	Пользователи домена	MRWXL	Все
FS01	D:\Share\Дистрибутивы\Антивирусы	Пользователи домена	RWXL	corp.local\Пользователи домена
FS01	D:\Share\Отдел HR	Пользователи домена	RXL	Все
FS01	D:\Share\Бухгалтерия	Пользователи домена	FMRWXL	Все

Анализ рисков в Active Directory

- 3 **административных** аккаунта с заданным **Service Principal Name** (SPN)
  - Уязвимость к перебору или атаке на понижение уровня шифрования, так как часто обладают несложными паролями

- 1 140 активных учетных записей с **бессрочным паролем**
  - Фактически неограниченный период медленного перебора пароля





Анализ рисков в Active Directory

- 4 654 **включенных неактивных** учетных записей

Уровень риска

Низкий Средний Высокий

Имя домена	Название OU	Пользователь/Группа	Имя учётной записи	Последняя авторизация
corp.local	Пользователи	corp.local\Ситников Юрий Ярославович	SitnikovYY	12/27/2013 5:31 AM
corp.local	Пользователи	corp.local\Федосеев Святослав Львович	FedoseevSL	12/27/2013 5:31 AM
corp.local	Пользователи	corp.local\Дроздов Наум Демьянович	DrozdovND	1/7/2014 5:30 AM
corp.local	Пользователи	corp.local\Большакова Олеся Иосифовна	BolshakovaOI	1/8/2014 5:30 AM

- 8 аккаунтов с включённым **делегированием аутентификации** по протоколу Kerberos

Уровень риска

Низкий Средний Высокий

Имя домена	Пользователь	Имя учётной записи	E-mail адрес
corp.local	corp.local\Гуляев Лев Витальевич	GulyaevLV	GulyaevLV@corp.local
corp.local	corp.local\Казакова Артемида Леонидовна	KazakovaAL	KazakovaAL@corp.local
corp.local	corp.local\Лапин Аркадий Яковович	LapinAY	LapinAY@corp.local

Поиск и классификация конфиденциальных данных

- **950+ млн** (950 534 645) файлов содержат конфиденциальные данные
- **339+ млн** (339 213 456) конфиденциальных документов доступны всем пользователям
- **50%** всех конфиденциальных данных хранятся в непредназначенных для этого местах хранения

Анализ рисков в Exchange

Уровень риска

Низкий Средний Высокий

- Права доступа в почтовые ящики руководства
  - почтовые ящики руководства и их содержимое доступны широкому кругу лиц или всем сотрудникам компании
  - администраторы могут использовать свои привилегии для чтения чужой почты

Путь доступа	Имя пользователя	Текущие разрешения
Mailbox Store\SavelevVM@corp.local\Входящие	Калинина Эльвира Парфеньевна	Полный доступ
Mailbox Store\SavelevVM@corp.local\Исходящие	Калинина Эльвира Парфеньевна	Полный доступ
Mailbox Store\SavelevVM@corp.local\Календарь	Калинина Эльвира Парфеньевна	Полный доступ
Mailbox Store\SavelevVM@corp.local\Календарь	Пестова Элла Кирилловна	Редактор
Mailbox Store\SorokinAR@corp.local\Контакты	Исаев Виталий Иванович	Владелец

VARONIS

Анализ рисков в Exchange

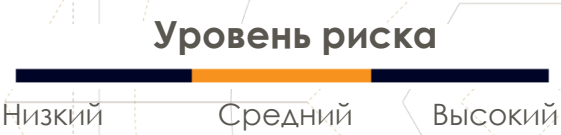
Уровень риска

Низкий Средний Высокий

- Аудит активности в почтовых ящиках других сотрудников:
  - отправка сообщений от лица коллеги
  - электронные письма руководства читаются и помечаются как непрочитанные нелегитимными пользователями без ведома владельца почтового ящика
  - удаление событий календаря, писем и т.д.

Время события	Кем выполнено	Путь	Объект	Описание события	Имя приложения
23/04/2019 13:41	corp.local\Калинина Эльвира Парфеньевна	Mailbox Store\SavelevVM@corp.local\Входящие	FW: Заседание управляющего совета	Сообщение открыто	
23/04/2019 13:42	corp.local\Калинина Эльвира Парфеньевна	Mailbox Store\SavelevVM@corp.local\Входящие	RE: Финансовый отчет за 1кв 2019	Сообщение открыто	Фин.отчет 1кв 2019.xlsx
23/04/2019 13:42	corp.local\Калинина Эльвира Парфеньевна	Mailbox Store\SavelevVM@corp.local\Исходящие	FW: Финансовый отчет за 1кв 2019	Сообщение отправлено на kalinina1979@mail.ru как corp.local\Савельев Владимир Михайлович	Фин.отчет 1кв 2019.xlsx
23/04/2019 18:57	corp.local\Администратор	Mailbox Store\MironovAL@corp.local\Входящие	FW: Вопросы по бюджетированию	Сообщение открыто	
23/04/2019 18:57	corp.local\Администратор	Mailbox Store\MironovAV@corp.local\Входящие	FW: Вопросы по бюджетированию	Сообщение помечено как непрочитанное	

Анализ устаревших данных



- **253 168 ГБ** устаревших данных
- **85+ млн.** (85 377 723) папок содержат только устаревшие, неиспользуемые данные
- **75%** проанализированной информации не модифицировалось в течение нескольких лет

- Объем устаревших данных
  - FS01 25%
  - FS03 22%
  - FS04 8%
  - SP_FS01 29%
- Из них содержащих конфиденциальные сведения
  - FS01 14%
  - FS03 11%
  - FS04 9%
  - SP_FS01 53%

О компании Varonis

- Varonis Systems – разработчик современных решений по кибербезопасности, основанных на **поведенческом анализе** пользователей и **защите данных** компании
- На рынке с **2005 года**. На российском рынке – с **2008 года**. С 2014 года – на бирже Nasdaq.
- Более **7000 клиентов** по всему миру

Coca-Cola TOYOTA John Hancock SEATTLE CANCER CARE ALLIANCE U.S.ARMY

> Клиенты Varonis всегда знают, где находятся их конфиденциальные данные, кто имеет к ним доступ и как они используются. В режиме реального времени они получают извещения об аномальной активности, кибератаках и событиях, которые могут привести к нарушению целостности данных или непрерывности бизнес-процессов.

VARONIS

Закажите бесплатный аудит рисков для вашей компании любым удобным вам способом:

Позвоните нам:

+7 (495)997-63-66

Напишите:

sales-russia@varonis.com