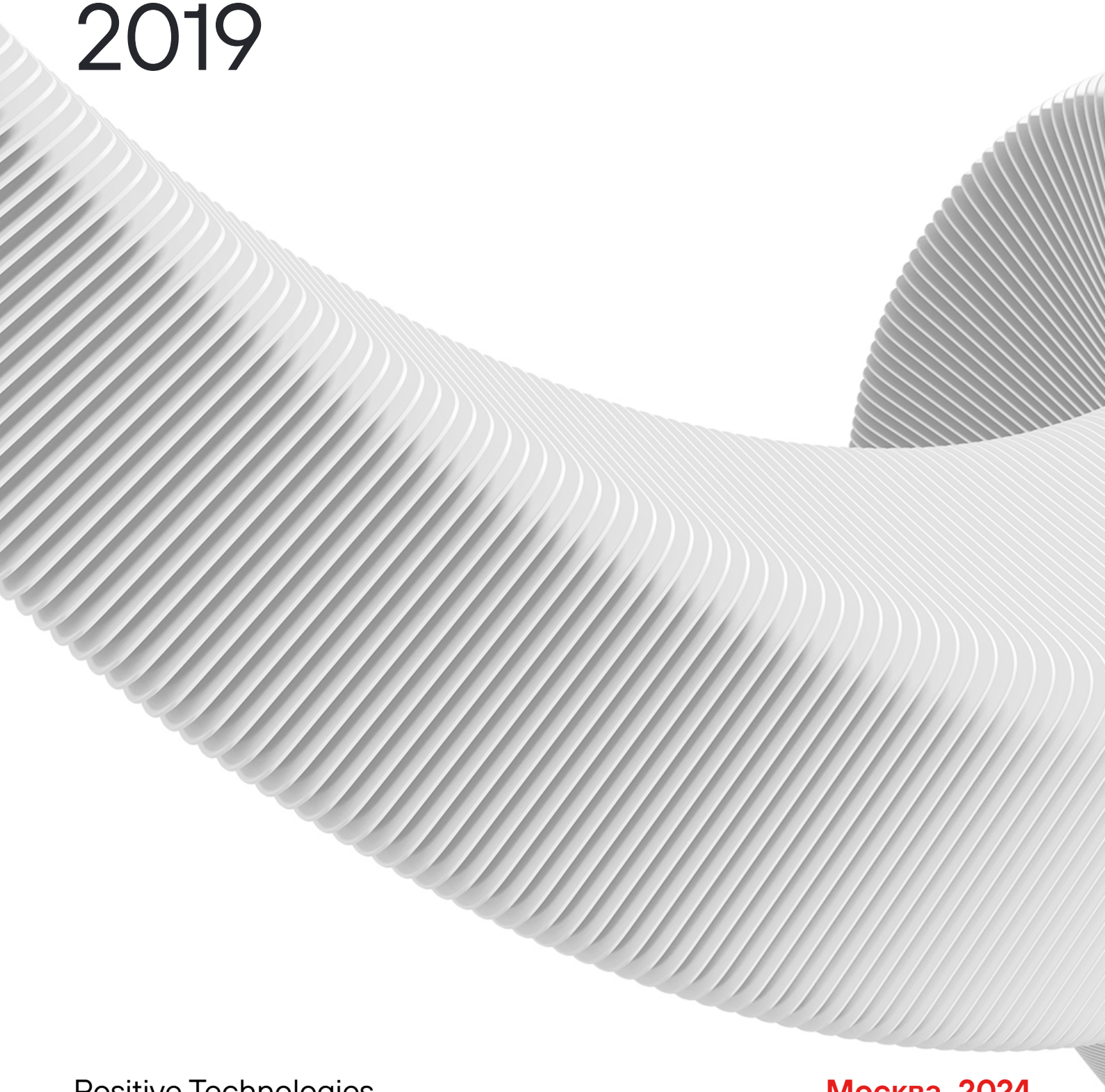
Руководство по защите Microsoft Exchange 2019



Positive Technologies

Москва, 2024

Содержание

1. Проблематика защиты Microsoft Exchange

1.1. Покрытие рынка

Согласно исследованию Microsoft, в 91% атак точкой входа или вектором атаки является электронная почта. Покрытие рынка Microsoft Exchange — не менее 70% для компаний более чем с 2000 пользователями, по мнению экспертов Positive Technologies.

Продукты и решения компании Microsoft уже давно завоевали популярность не только у частных пользователей, но и у государственных и коммерческих организаций. Одним из таких решений является сервис Microsoft Exchange. Он располагается на сетевом периметре организации и предназначен для отправки сообщений и коммуникации как внутри компании, так и с внешними пользователями, что делает его одним из ключевых инструментов для ведения операционной деятельности. Однако расположение сервиса автоматически привлекает внимание хакеров, а широкая популярность делает проблему обеспечения его безопасности массовой.

Этот документ описывает типовые проблемы безопасности почтовой системы на базе Microsoft Exchange и дает рекомендации по повышению защищенности.

1.2. Статистика по уязвимостям

База уязвимостей MaxPatrol VM содержит информацию о 171 уязвимости Microsoft Exchange. Из них 50 уязвимостей имеют оценку по шкале CVSS v3 более 7 баллов. Исходя из этой статистики, видно, что в Microsoft Exchange периодически появляются критически опасные уязвимости.

1.3. Архитектурные особенности

Microsoft Exchange 2019 по умолчанию интегрируется с Active Directory. Поэтому взлом Microsoft Exchange может привести к получению привилегий администратора домена Active Directory. Кроме того, целью злоумышленника могут являться данные в Microsoft Exchange.

Таким образом, Microsoft Exchange может являться как ключевой, так и целевой системой, что делает его одной из главных и легких целей для злоумышленника.

2. Недопустимые события Microsoft Exchange 2019

Для примера в качестве недопустимых событий возьмем:

- доступ к деловой переписке топ-менеджмента компании, которая хранится в Microsoft Exchange;
- массовая рассылка нелегитимного контента по всем контрагентам.

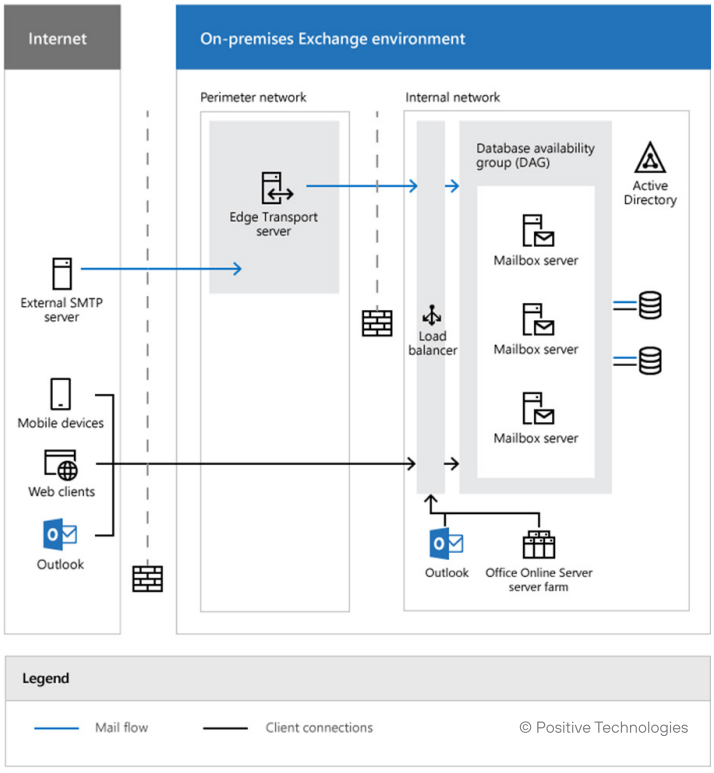
3. Пример типовой инсталляции Microsoft Exchange 2019

В этом разделе приведен пример типовой инсталляции почтовой системы на базе Microsoft Exchange Server 2019 в компании (организации) с количеством пользователей от 1000 до 5000.

3.1. Архитектурная схема типовой инсталляции

Архитектурная схема типовой инсталляции почтовой системы на базе Microsoft Exchange Server 2019 представлена на рисунке 1.

Рисунок 1. Архитектурная схема типовой инсталляции почтовой системы



Более общая референсная архитектурная схема представлена на сайте Microsoft по ссылке: https://techcommunity.microsoft.com/t5/exchange-team-blog/exchange-server-2016-architecture/ba-p/603598.

3.2. Описание типовой инсталляции

Почтовая система на базе Exchange использует серверы почтовых ящиков и пограничные транспортные серверы.

Серверы почтовых ящиков содержат:

- службы транспорта для маршрутизации электронной почты;
- базы данных почтовых ящиков для обработки, предоставления и хранения данных;
- службы клиентского доступа, которые принимают клиентские подключения для всех протоколов. Внешние такие службы отвечают за маршрутизацию (проксирование) подключений к соответствующим внутренним службам на сервере почтовых ящиков. Виртуальные каталоги для внутренних служб настроены на серверах почтовых ящиков.

Управление серверами почтовых ящиков осуществляется с помощью центра администрирования Exchange (EAC) и командной консоли Exchange.

Пограничные транспортные серверы отвечают за поток обработки внешней почты в организации Exchange.

Пограничные транспортные серверы, как правило, устанавливаются в сети периметра и подписываются на внутреннюю организацию Exchange. Благодаря процессу синхронизации EdgeSync сведения о получателе и другие данные конфигурации становятся доступными для пограничного транспортного сервера, когда электронные сообщения поступают в организацию Exchange и покидают ее.

Пограничные транспортные серверы предоставляют правила защиты от нежелательной почты и потока обработки почты, когда почта входит в организацию Exchange и покидает ее.

Управление пограничными транспортными серверами выполняется с помощью командной консоли Exchange.

Office Online Server используется для предварительного просмотра документов в Outlook on the web.

Группа доступности базы данных (DAG) — это основной элемент платформы обеспечения высокой доступности и устойчивости сайта, встроенной в Exchange Server. DAG — это группа серверов почтовых ящиков, на которых размещается набор баз данных и обеспечивается автоматическое восстановление на уровне базы данных из-за сбоев базы данных, сети и сервера.

Службы клиентского доступа на серверах почтовых ящиков Exchange отвечают за прием всех форм клиентских подключений. Службы клиентского доступа (внешний интерфейс) поддерживают эти подключения к внутренним службам на целевом сервере почтовых ящиков (локальном или удаленном сервере почтовых ящиков, на котором хранится активная копия почтового ящика пользователя). Клиенты не подключаются к внутренним службам напрямую.

Используемый клиентом протокол определяет протокол, с помощью которого запрос проксируется к внутренним службам на целевом сервере почтовых ящиков. Например, если клиент подключился с помощью протокола HTTP, сервер почтовых ящиков использует этот протокол для проксирования запроса на целевой сервер почтовых ящиков (защищенный с помощью самоподписанного SSL-сертификата). Если протокол клиента это IMAP или POP, то используется один из двух этих протоколов.

MAPI по протоколу HTTP используется по умолчанию для подключений Outlook: этот протокол предоставляет дополнительные элементы управления, такие как возможность включения или отключения MAPI по протоколу HTTP для каждого пользователя и объявления его для внешних клиентов.

4. Проблемы безопасности типовой инсталляции

В этом разделе приведены проблемы безопасности типовой инсталляции почтовой системы на базе Microsoft Exchange Server 2019.

Типовая инсталляция почтовой системы зачастую обладает следующими проблемами с точки зрения безопасности:

- отсутствует процесс регулярного тестирования и установки обновлений для операционных систем и ПО почтовой системы;
- учетная запись, под которой осуществлялась установка Exchange, продолжает находиться в группах, обладающих повышенными привилегиями в домене Active Directory;
- административные учетные записи почтовой системы не используют механизмы строгой аутентификации;
- пользователи почтовой системы используют устаревшие протоколы аутентификации (NTLM v1);
- служебные учетные записи почтовой системы обладают правами подключения по любым протоколам;
- используются устаревшие алгоритмы шифрования сетевого трафика почтовой системы (DES, RC4) и устаревшие протоколы сетевого доступа (TLS 1.0, SMB v1);
- серверы почтовой системы предоставляют информацию о версиях используемых компонентов;
- сетевое взаимодействие из интернета осуществляется напрямую с серверами почтовой системы, расположенными во внутренней сети.

Для типовой инсталляции почтовой системы на базе Exchange могут быть применены 14 тактик и более 160 техник из матрицы MITRE ATT&CK.

Для применения этих техник атакующему достаточно иметь квалификацию «Киберхулиган/Энтузиаст-одиночка».

В рамках тактики «Разведка» могут быть применены следующие техники:

- T1589 Сбор информации об атакуемых пользователях;
- T1590 Сбор информации об атакуемой сетевой инфраструктуре;
- T1591 Сбор бизнес-информации об атакуемой организации;
- T1592 Сбор информации об атакуемых узлах;
- T1593 Поиск на общедоступных сайтах;
- T1594 Поиск на сайтах атакуемой организации;
- T1595 Активное сканирование;
- T1596 Поиск технической информации в общедоступных источниках;
- T1597 Поиск в закрытых источниках;
- T1598 Фишинг с целью сбора сведений.

В рамках тактики «Подготовка ресурсов» могут быть применены следующие техники:

- T1583 Приобретение инфраструктуры;
- T1584 Компрометация сторонней инфраструктуры;
- T1585 Создание учетных записей;
- T1586 Компрометация учетных записей;
- T1587 Разработка собственных средств;
- T1588 Подготовка необходимых средств;
- T1608 Размещение средств;
- T1650 Приобретение доступа.

В рамках тактики «Первоначальный доступ» могут быть применены следующие техники:

- T1078 Существующие учетные записи;
- T1091 Распространение через съемные носители;
- T1190 Недостатки в общедоступном приложении;
- T1195 Компрометация цепочки поставок;
- T1199 Доверительные отношения;
- T1566 Фишинг.

В рамках тактики «Выполнение» могут быть применены следующие техники:

- T1047 Инструментарий управления Windows;
- T1053 Запланированная задача (задание);
- T1059 Интерпретаторы командной строки и сценариев;
- T1072 Средства развертывания ПО;
- T1106 Нативный API;
- T1129 Общие модули;
- T1203 Эксплуатация уязвимостей в клиентском ПО;
- T1204 Выполнение с участием пользователя;
- T1569 Системные службы.

В рамках тактики «Закрепление» могут быть применены следующие техники:

- T1037 Сценарии инициализации при загрузке или входе в систему;
- T1053 Запланированная задача (задание);
- T1078 Существующие учетные записи;
- T1098 Манипуляции с учетной записью;
- T1136 Создание учетной записи;
- T1197 Задания BITS;
- T1205 Передача управляющих сигналов в трафике;
- T1505 Компонент серверного ПО;
- T1547 Автозапуск при загрузке или входе в систему;
- T1556 Изменение процесса аутентификации;
- T1574 Перехват потока исполнения.

В рамках тактики «Повышение привилегий» могут быть применены следующие техники:

- T1037 Сценарии инициализации при загрузке или входе в систему;
- T1053 Запланированная задача (задание);
- T1055 Внедрение кода в процессы;
- T1068 Эксплуатация уязвимостей для повышения привилегий;
- T1078 Существующие учетные записи;
- T1134 Манипуляции с токенами доступа;
- T1484 Изменение доменной политики;
- T1547 Автозапуск при загрузке или входе в систему;
- T1548 Обход механизмов контроля привилегий;
- T1574 Перехват потока исполнения.

В рамках тактики «Предотвращение обнаружения» могут быть применены следующие техники:

- T1006 Прямой доступ к тому;
- T1014 Руткит;
- T1027 Обфусцированные файлы или данные;
- T1036 Маскировка;
- T1055 Внедрение кода в процессы;
- T1070 Устранение индикаторов;
- T1078 Существующие учетные записи;
- T1112 Изменение реестра;
- T1127 Выполнение через доверенные утилиты разработчика;
- T1134 Манипуляции с токенами доступа;
- T1140 Деобфускация/декодирование файлов или данных;
- T1197 Задания BITS;
- T1202 Непрямое выполнение команд;
- T1205 Передача управляющих сигналов в трафике;
- T1207 Поддельный контроллер домена;
- T1211 Эксплуатация уязвимостей для предотвращения обнаружения;
- T1216 Выполнение через системный сценарий;
- T1218 Выполнение с помощью системных бинарных файлов;
- T1222 Изменение разрешений для файлов и каталогов;
- T1480 Ограничения на исполнение;
- T1484 Изменение доменной политики;
- T1548 Обход механизмов контроля привилегий;
- T1550 Использование альтернативных сущностей для аутентификации;
- T1553 Нарушение работы средств контроля доверия;
- T1556 Изменение процесса аутентификации;
- T1562 Ослабление защиты;
- T1564 Сокрытие артефактов;
- T1574 Перехват потока исполнения;
- T1599 Преодоление границ сети;
- T1600 Понижение надежности шифрования;
- T1622 Предотвращение отладки.

В рамках тактики «Получение учетных данных» могут быть применены следующие техники:

- T1003 Получение дампа учетных данных;
- T1040 Прослушивание сетевого трафика;
- T1056 Перехват вводимых данных;
- T1110 Метод перебора;
- T1187 Принудительная аутентификация;
- T1212 Эксплуатация уязвимостей для получения учетных данных;
- T1528 Кража токена доступа к приложению;
- T1539 Кража сессионных куки;
- T1552 Незащищенные учетные данные;
- T1555 Учетные данные из хранилищ паролей;
- T1556 Изменение процесса аутентификации;
- T1557 «Злоумышленник посередине»;
- T1558 Кража или подделка билетов Kerberos;
- T1606 Подделка учетных данных для веб-ресурсов.

В рамках тактики «Изучение» могут быть применены следующие техники:

- T1007 Изучение системных служб;
- T1010 Изучение открытых приложений;
- T1012 Запросы к реестру;
- T1016 Изучение конфигурации сети;
- T1018 Изучение удаленных систем;
- T1033 Изучение владельца или пользователей системы;
- T1040 Прослушивание сетевого трафика;
- T1046 Изучение сетевых служб;
- T1049 Изучение сетевых подключений;
- T1057 Изучение процессов;
- T1069 Изучение групп разрешений;
- T1082 Изучение системы;
- T1083 Изучение файлов и каталогов;
- T1087 Изучение учетных записей;
- T1124 Изучение системного времени;
- T1135 Изучение общих сетевых ресурсов;
- T1201 Изучение парольной политики;
- T1482 Изучение доверительных отношений между доменами;
- T1518 Изучение установленного ПО;
- T1615 Изучение групповой политики;
- T1622 Предотвращение отладки;
- T1652 Изучение драйверов устройств.

В рамках тактики «Перемещение внутри периметра» могут быть применены следующие техники:

- T1080 Заражение общего содержимого;
- T1210 Эксплуатация уязвимостей в удаленных службах;
- T1534 Внутренний целевой фишинг;
- T1550 Использование альтернативных сущностей для аутентификации;
- T1570 Передача инструментов внутри периметра.

В рамках тактики «Сбор данных» могут быть применены следующие техники:

- T1005 Данные из локальной системы;
- T1039 Данные с общих сетевых дисков;
- T1056 Перехват вводимых данных;
- T1074 Промежуточное хранение данных;
- T1114 Сбор электронной почты;
- T1119 Автоматизированный сбор данных;
- T1557 «Злоумышленник посередине»;
- T1560 Архивация собранных данных.

В рамках тактики «Организация управления» могут быть применены следующие техники:

- T1001 Обфускация данных;
- T1008 Резервные каналы;
- T1071 Протокол прикладного уровня;
- T1090 Прокси-сервер;
- T1095 Протоколы (кроме прикладного уровня);
- T1102 Веб-служба;
- T1104 Отдельный канал для каждого этапа;
- T1105 Передача инструментов из внешней сети;
- T1132 Кодирование данных;
- T1205 Передача управляющих сигналов в трафике;
- T1219 ПО для удаленного доступа;
- T1568 Динамическое разрешение;
- T1571 Нестандартный порт;
- T1572 Туннелирование протокола;
- T1573 Зашифрованный канал.

В рамках тактики «Эксфильтрация данных» могут быть применены следующие техники:

- T1011 Эксфильтрация через альтернативную сетевую среду;
- T1020 Автоматизированная эксфильтрация;
- T1029 Передача по расписанию;
- T1030 Ограничение размера передаваемых блоков данных;
- T1041 Эксфильтрация по каналу управления;
- T1048 Эксфильтрация по альтернативному протоколу;
- T1567 Эксфильтрация через веб-службу.

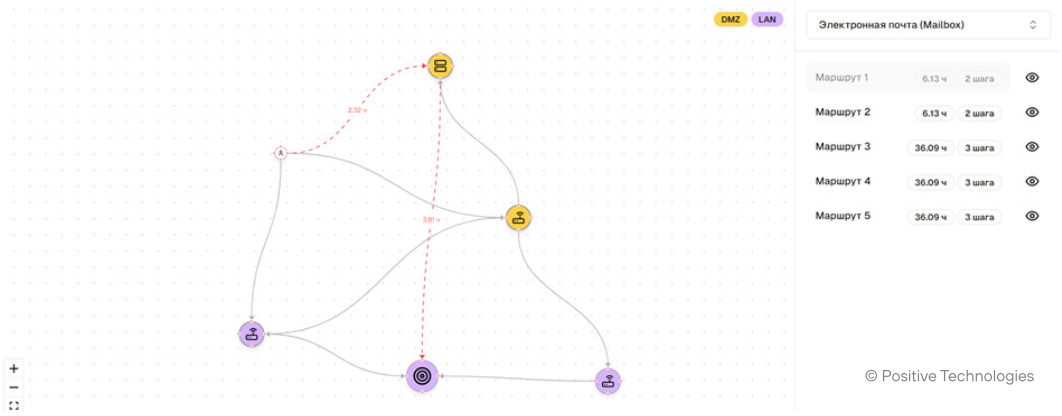
В рамках тактики «Деструктивное воздействие» могут быть применены следующие техники:

- T1485 Уничтожение данных;
- T1486 Шифрование данных;
- T1489 Остановка службы;
- T1490 Препятствование восстановлению системы;
- T1496 Несанкционированное использование ресурсов;
- T1498 Сетевой отказ в обслуживании;
- T1499 Точечный отказ в обслуживании;
- T1529 Завершение работы или перезагрузка системы;
- T1531 Прекращение доступа к учетной записи;
- T1561 Уничтожение диска;
- T1565 Манипуляции с данными.

5. Расчет времени проникновения для инсталляции с параметрами по умолчанию

При параметрах настройки по умолчанию только 2 из 43 превентивных контролей были реализованы, что значительно облегчает злоумышленнику реализацию недопустимых событий. Злоумышленнику может потребоваться всего два шага и около 6 часов на реализацию недопустимого события (см. рисунок 2):

Рисунок 2. Путь атакующего до повышения защищенности



6. Рекомендации по повышению защищенности

В этом разделе приведены рекомендации по повышению защищенности инсталляции почтовой системы на базе Microsoft Exchange Server 2019.

Соответствие рекомендаций защитным мерам из матрицы MITRE ATT&CK приведены в таблице 1.

Подробные описания рекомендаций приведены в подразделах ниже.

Таблица 1. Соответствие рекомендаций защитным мерам из матрицы MITRE ATT&CK

Рекомендация	Защитные меры из матрицы MITRE ATT&CK
Обновление Exchange Server и установка последних обновлений CU и SU	M1051 Update Software
Ограничения административной учетной записи Exchange	M1026 Privileged Account Management
Настройка аутентификации по сертификатам для учетных записей сотрудников с правами администратора	M1036 Account Use Policies M1043 Credential Access Protection M1032 Multi-factor Authentication
Настройка службы Kerberos для аутентификации в локальной сети	M1043 Credential Access Protection
Отключение OWA, ActiveSync для служебных учетных записей	M1036 Account Use Policies
Усиление парольной политики для учетных записей	M1027 Password Policies
Изменение конфигурации протоколов SSL и TLS	M1041 Encrypt Sensitive Information
Отключение SMB v1	M1042 Disable or Remove Feature or Program
Скрытие заголовков ответа сервера Microsoft IIS	M1054 Software Configuration
Расширенная защита Windows	M1043 Credential Access Protection
Использование серверов с ролью Edge Transport	M1049 Antivirus/Antimalware M1030 Network Segmentation
Ограничения для почтовых клиентов	M1043 Credential Access Protection M1037 Filter Network Traffic M1035 Limit Access to Resource Over Network M1032 Multi-factor Authentication M1031 Network Intrusion Prevention M1030 Network Segmentation M1020 SSL/TLS Inspection

6.1. Обновление Exchange Server и установка последних обновлений CU и SU

Используйте только поддерживаемые производителем версии ПО, а также следите за выпуском новых версий накопительных обновлений (CU) и обновлений безопасности (SU). Эти обновления содержат в себе исправления программных ошибок и закрывают уязвимости, которые были обнаружены в ходе эксплуатации. Узнать больше о построении процесса управления уязвимостями можно на нашем курсе-практикуме: vm.edu.ptsecurity.com.

6.2. Ограничения административной учетной записи Exchange

Убедитесь, что административная учетная запись Microsoft Exchange не является членом следующих групп:

- Администратор домена (Domain Admin);
- Администратор предприятия (Enterprise Admin);
- Администратор схемы (Schema Admin).

> **ВАЖНО! Допускается ВРЕМЕННО включать административную учетную запись Microsoft Exchange в указанные выше группы во время:**

- первоначальной установки Microsoft Exchange;
- миграции службы Microsoft Exchange на более новую версию.

6.3. Настройка аутентификации по сертификатам для учетных записей сотрудников с правами администратора

1. Настройте внутреннюю инфраструктуру PKI согласно документации Microsoft: https://learn.microsoft.com/en-us/windows-server/identity/ad-cs.
2. Для администрирования Microsoft Exchange создайте отдельные учетные записи.
3. Выпишите для выделенных учетных записей сертификаты для аутентификации. Требования к сертификатам описаны по ссылке: https://learn.microsoft.com/en-us/windows/security/identity-protection/smart-cards/smart-card-certificate-requirements-and-enumeration.
4. Настройте для выделенных учетных записей вход только с использованием смарт-карт. В качестве смарт-карт можно использовать USB-токены JaCarta PKI или аналогичные.
5. Настройте аутентификацию по сертификатам для доступа к Exchange Admin Center согласно инструкции Microsoft, доступной по ссылке: https://learn.microsoft.com/en-us/exchange/plan-and-deploy/post-installation-tasks/configure-certificate-based-auth?view=exchserver-2019.

6.4. Настройка службы Kerberos для аутентификации в локальной сети

Настройте аутентификацию для клиентов Microsoft Outlook и OWA (Outlook Anywhere) в локальной сети согласно инструкции, доступной по ссылке: https://learn.microsoft.com/en-us/exchange/architecture/client-access/kerberos-auth-for-load-balanced-client-access?view=exchserver-2019.

6.5. Отключение OWA и ActiveSync для служебных учетных записей

Отключите сервисы OWA и ActiveSync для служебных учетных записей. Служебная (сервисная) учетная запись — любая учетная запись, не связанная с конкретным физическим лицом (сотрудником компании или подрядчиком). Примерами таких учетных записей являются:

- учетные записи для отправки или получения уведомлений от систем мониторинга;
- учетные записи, используемые для запуска служб с ограниченными правами.

Отключить OWA и ActiveSync для конкретной учетной записи можно:

- из графического интерфейса согласно инструкции, доступной по ссылке: https://learn.microsoft.com/en-us/exchange/clients/exchange-activesync/activesync-mailbox-access?view=exchserver-2019#use-the-exchange-management-shell-to-enable-or-disable-exchange-activesync-access-to-a-mailbox;
- из командной строки с помощью команд:
  - Set-CasMailbox -Identity <MailboxIdentity> -ActiveSyncEnabled $false
  - Set-CasMailbox -Identity <MailboxIdentity> -OWAEnabled $false

6.6. Усиление парольной политики для учетных записей

Используйте парольные политики для определения требований к сложности паролей, частоте смены паролей и параметрам блокировки учетной записи.

Рекомендуемая минимальная длина пароля — 12 знаков. В пароле должны быть как минимум три из четырех групп знаков.

На текущий момент нет однозначного мнения, каким должен быть максимальный срок действия пароля. При слишком коротком сроке действия повышается нагрузка на подразделение, занимающееся поддержкой ИТ-инфраструктуры, так как очень часто смена пароля приводит к блокировке учетной записи пользователя.

Типовые причины блокировки при смене пароля:

- пользователь забыл сменить пароль на одном из своих устройств или в одном из приложений;
- ошибки используемого ПО, которое некорректно обрабатывают ситуацию смены пароля.

При слишком большом сроке увеличивается вероятность использования паролей, полученных в результате публичных утечек. Чаще всего срок действия пароля устанавливается в диапазоне от 40 до 180 дней. Решение о максимальном сроке действия пароля предлагается принимать исходя из условий и особенностей деятельности конкретной организации.

Пороговое значение блокировки рекомендуется подбирать экспериментально в диапазоне от пяти до десяти попыток аутентификации, ориентируясь на количество запросов пользователей в техническую поддержку по поводу блокировки учетной записи.

6.7. Изменение конфигурации протоколов SSL и TLS

Выполните рекомендации Microsoft по конфигурированию протоколов SSL и TLS, доступные по сылке: https://learn.microsoft.com/en-us/exchange/exchange-tls-configuration?view=exchserver-2019.

Используйте RSA-2048 при создании новых ключей сертификатов. При обновлении или создании новых запросов на подпись сертификатов рекомендуется отдавать предпочтение алгоритму SHA-256 или более безопасным.

При создании самоподписанных сертификатов следуйте рекомендациям Microsoft, доступным по ссылке: https://learn.microsoft.com/en-us/exchange/architecture/client-access/certificates?source=recommendations&view=exchserver-2019.

6.8. Отключение SMB v1

С помощью команд PowerShell проверьте, отключен ли на серверах протокол SMB v1. Для Windows 2012 R2 и выше используйте следующие команды:

- Get-WindowsFeature FS-SMB1).Installed
- Get-SmbServerConfiguration \| Select EnableSMB1Protocol

Значение True в полученном результате выполнения команды означает, что протокол SMB v1 включен.

ВАЖНО! Перед отключением SMB v1 убедитесь, что witness-сервер DAG поддерживает как минимум протокол SMB v2 и ваш DAG корректно сконфигурирован.

Проверить правильность конфигурации DAG можно по инструкции Microsoft, доступной по ссылке: https://learn.microsoft.com/en-us/exchange/high-availability/manage-ha/manage-dags?view=exchserver-2019.

Отключить протокол SMB v1 можно двумя способами:

- С помощью команд (для Windows 2012 R2 и выше):
  - Disable-WindowsOptionalFeature -Online -FeatureName smb1protocol
  - Set-SmbServerConfiguration -EnableSMB1Protocol $false
- С использованием групповых политик по инструкции Microsoft, доступной по ссылке: https://learn.microsoft.com/en-us/windows-server/storage/fileserver/troubleshoot/detect-enable-and-disable-smbv1-v2-v3.

6.9. Скрытие заголовков ответа сервера Microsoft IIS

Скройте отображение заголовков ответов X-AspNet-Version, X-Powered-By и Server, содержащих номера версий веб-приложений. Чтобы убрать отображение заголовка X-AspNet-Version:

1. Откройте в Microsoft IIS Manager параметры сервера (Configuration Editor).
2. Выберите секцию system.web/httpRuntime.
3. В поле enableVersionHeader смените True на False.

Заголовок X-Powered-By является настраиваемым. Чтобы заменить его содержимое:

1. Откройте параметры Microsoft IIS Manager.
2. Выберите пункт HTTP Response Header.
3. Выберите пункт X-Powered-By и измените значение поля Value на произвольное.

Заголовок Server раскрывает версию сервера Microsoft IIS. Скрыть эту информацию можно с помощью компонента URL Rewrite. Необходимо создать правило типа Outbound, заполнив поля в соответствии с таблицей 2.

Таблица 2. Пример параметров правила типа Outbound компонента URL Rewrite

Параметр	Значение
NAME	**HIDE IIS VERSION**
MATCHING SCOPE	SERVER VARIABLE
VARIABLE NAME	**RESPONSE_SERVER**
VARIABLE VALUE	MATCHES THE PATTERN
USING	REGULAR EXPRESSIONS
PATTERN	.+
ACTION TYPE	REWRITE
VALUE ANY	**ANY**

В таблице жирным шрифтом выделены значения, которые могут заполняться произвольно.

6.10. Расширенная защита Windows

Включите расширенную защиту (Extended Protection) системы Windows, в том числе для всех виртуальных каталогов Microsoft Exchange Server.

Расширенная защита Windows поддерживается в Microsoft Exchange Server 2013, 2016 и 2019, а также начиная с выпусков Microsoft Exchange Server Security Update (SU) за август 2022 года. При этом имеются следующие ограничения:

- Расширенная защита поддерживается только в Microsoft Exchange Server 2013 CU23, Microsoft Exchange Server 2016 CU22 и Microsoft Exchange Server 2019 CU11 или более поздней версии с установленными обновлениями безопасности за август 2022 года.
- Расширенную защиту нельзя включить на серверах Microsoft Exchange Server 2013 с общими папками в среде сосуществования. После включения расширенной защиты, если в Microsoft Exchange 2013 есть общедоступные папки, они больше не будут отображаться для конечных пользователей.
- Расширенную защиту нельзя включить в Microsoft Exchange Server 2016 CU22, Microsoft Exchange Server 2019 CU11 или более ранней версии, на которой размещена иерархия общих папок.
- Расширенная защита не работает с серверами, использующими метод Hybrid Modern Authentication. Включение расширенной защиты на серверах, использующих метод Hybrid Modern Authentication, приведет к нарушению работы отдельных функций, таких как миграция почтовых ящиков и сведения о доступности.
- При включенной расширенной защите не поддерживается протокол NTLM v1.
- Конфигурация протокола TLS должна быть согласована на всех серверах Microsoft Exchange.

ВАЖНО! Если клиент будет использовать протокол NTLM v1 вместо NTLM v2 и на сервере Microsoft Exchange будет включена расширенная защита, это приведет к запросам пароля на стороне клиента без возможности успешной аутентификации в Microsoft Exchange. Выбрать тип аутентификации и переключиться на протокол NTLM v2 можно с помощью внесения изменений в политику доменов через реестр:

- Групповая политика: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\[Network security: LAN Manager authentication level].
- Ключ реестра: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa.
- Значение реестра: LmCompatibilityLevel.
- Рекомендованное значение: отправлять только ответ NTLM v2. Отказаться от LM и NTLM (значение ключа реестра — 5).

6.11. Использование серверов с ролью Edge Transport

Ознакомьтесь с архитектурой Microsoft Exchange (см. схему On-premises Exchange 2016 environment по ссылке: https://learn.microsoft.com/en-us/exchange/architecture/architecture?view=exchserver-2019).

Используйте серверы с ролью Edge Transport:

- если вы не используете сторонние антиспам- и антифишинг-средства и планируете использовать только встроенные возможности Microsoft Exchange для противодействия спаму и фишингу;
- если сторонние антиспам- и антифишинг-средства требуют для установки серверы с ролью Edge Transport.

В остальных случаях достаточно будет настроить программное обеспечение Postfix для взаимодействия с внешними почтовыми системами.

ВАЖНО! Не допускается публикация на сетевом периметре серверов с ролью Mailbox.

6.12. Ограничения для почтовых клиентов

Заблокируйте на внешнем периметре доступ по протоколу MAPI over HTTP. Порт по умолчанию — 443 (TCP). Подключение почтовых клиентов Microsoft Outlook должно быть разрешено только:

- из локальной проводной сети организации;
- через VPN-сервис.

Запретите подключение мобильных клиентов по протоколу ActiveSync без VPN. При необходимости использовать мобильные клиенты, не подключенные к VPN, по протоколу ActiveSync используйте аутентификацию по сертификатам.

Сделайте Outlook on the web доступным только после подключения к VPN и запретите доступ через интернет.

При необходимости опубликовать Outlook on the web на внешнем периметре и сделать доступным через интернет, опубликуйте Outlook on the web через Web Application Proxy и настройте многофакторную аутентификацию. Дополнительно рекомендуется временно блокировать IP-адрес атакующего после нескольких неудачных попыток входа.

Проверьте, выключены ли у вас протоколы IMAP4 и POP3 на серверах. По умолчанию эти протоколы выключены. Подробная информация доступна по ссылке: https://learn.microsoft.com/en-us/exchange/clients/pop3-and-imap4/pop3-and-imap4?view=exchserver-2019.

Если протоколы IMAP4 и POP3 включены, отключите их согласно инструкции, доступной по ссылке: https://learn.microsoft.com/en-us/exchange/clients/pop3-and-imap4/configure-pop3?view=exchserver-2019.

Если протоколы IMAP4 и POP3 необходимо использовать, заблокируйте на внешнем периметре доступ через интернет по этим протоколам и разрешите подключение к ним только:

- из локальной проводной сети организации;
- через VPN-сервис.

7. Расчет времени проникновения (TTA) после применения рекомендаций

После применения рекомендаций количество реализованных превентивных контролей возросло до 21 из 43. Благодаря этому расчетное TTA увеличилось более чем в 10 раз — до 64,47 часов (см. рисунок 3 и рисунок 4).

Рисунок 3. Путь атакующего после применения рекомендаций

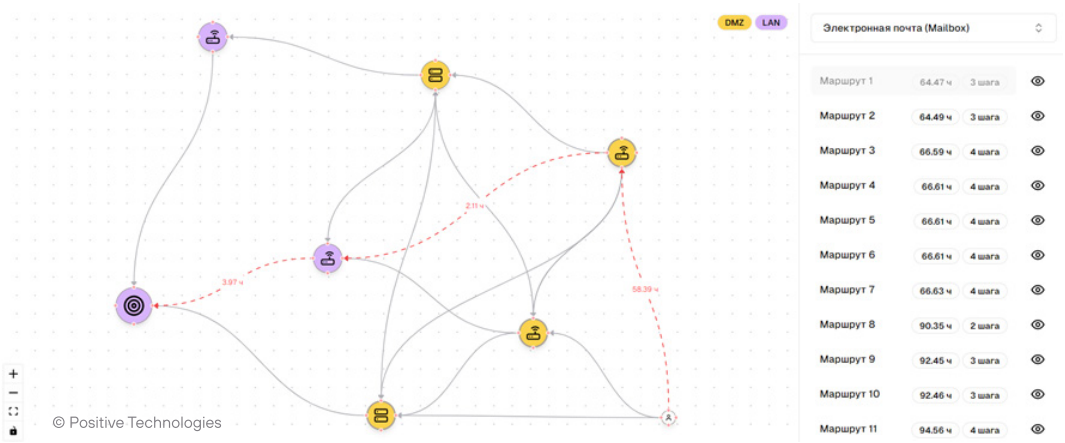


Рисунок 4. Путь атакующего с детализацией по техникам

8. Заключение

Несмотря на то что путь злоумышленника не удалось удлинить за счет повышения защищенности, выполнение каждого шага будет занимать у него значительно больше времени, а значит у команды мониторинга и реагирования будет намного больше времени на детектирование и локализацию действий злоумышленника.

При этом реализация контролей не требовала дополнительных затрат на внедрение новых средств защиты, и большинство из них может быть применено в течение нескольких часов.

ptsecurity.com
pr@ptsecurity.com