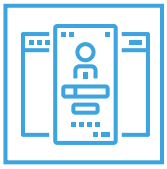
КОМПЛЕКСНАЯ БЕЗОПАСНОСТЬ С РЕШЕНИЯМИ MICROSOFT

Информзащита
Системный интегратор

Компания Информзащита предлагает внедрить меры для безопасного удаленного доступа на базе решений Microsoft



Multifactor Authorization – многоуровневый подход к авторизации

- Обойти несколько факторов проверки подлинности представляет нетривиальную задачу для злоумышленников
- Если злоумышленник заполучил пароль пользователя, им нельзя воспользоваться без дополнительной проверки подлинности

Conditional Access – условный доступ (политики безопасности)

- Средство, используемое Azure Active Directory для контроля доступа и применения политик организации
- Условия доступа: платформа устройства с которой выполняется вход, пользователь и расположение откуда выполняется вход, используемое приложение, риск входа в реальном времени
- В зависимости от выполнения условий применяются политики: разрешения, блокировки доступа, требования MFA, использование определенных приложений

Microsoft Intune – облачная служба управления

- **Основное внимание уделяется: ноутбукам**, мобильным устройствам (MDM) и мобильным приложениям (MAM)
- Интегрируется с Microsoft 365 и Azure Active Directory (Azure AD) для контроля доступа для пользователей и доступа к продуктам
- Интегрируется с Azure Information Protection для защиты данных
- При использовании совместно с Microsoft 365 все сотрудники могут эффективно работать на всех устройствах с одновременной защитой для данной организации

Microsoft Teams

- Единое пространство для общения: чат, собрание, звонки, совместная работа над проектами
- Есть возможность работать с документами прямо в Teams
- Организовано надежное хранение файлов там с контролируемым доступом
- Teams позволяет быстро присоединяться к звонкам или встречам

Информзащита
Системный интегратор

Azure AD Application Proxy

- Поддержка многофакторной проверки подлинности для облачных и локальных приложений
- Безопасный удаленный доступ к веб-приложениям, размещенным в локальной среде, и постоянная защита корпоративных ресурсов
- Интеграция с современными методами аутентификации и облачными технологиями, в том числе с приложениями SaaS и поставщиками удостоверений
- Не нужно изменять или обновлять приложения для работы и открывать входящие подключения через брандмауэр
- Пользователи получают доступ к облачным или локальным приложениям откуда угодно

Office 365 Advanced Treat Protection

- Защищает организацию от угроз, которые могут представлять электронные сообщения, ссылки (URL-адреса) и средства совместной работы.

ATP включает:

Политики защиты от угроз

Определите политики защиты от угроз, чтобы задать необходимый уровень защиты для организации.

Отчеты

Просматривайте отчеты в режиме реального времени, чтобы отслеживать производительность ATP в организации.

Анализ угроз и реагирование на них

Используйте передовые инструменты для анализа, изучения, моделирования и предотвращения угроз.

Автоматизированный анализ угроз и реагирование на них

Экономьте время и усилия при анализе и устранении угроз.

Office 365 ATP план 1 включает:

- ✓ Безопасные вложения
- ✓ Безопасные ссылки
- ✓ ATP для SharePoint, OneDrive, Microsoft Teams и Office ProPlus
- ✓ Расширенная защита от фишинга
- ✓ Обнаружение в режиме реального времени

Политики защиты от угроз состоят из:

- ✓ Безопасные вложения ATP.
  Защита системы обмена сообщениями от угроз нулевого дня путем проверки вложений в сообщениях электронной почты на наличие вредоносного содержимого.
- ✓ Безопасные ссылки ATP.
  Проверка URL-адресов (например, в сообщениях электронной почты и файлах Office) в момент щелчка по ним. Защита будет действовать и в среде обмена сообщениями, и в среде Office. Ссылки сканируются при каждой попытке перехода.

Информзащита
Системный интегратор

Office 365 ATP **план 2**

включает план 1 и плюс:

- ✓ Журналы учета угроз
- ✓ Обозреватель угроз
- ✓ Автоматизированный анализ угроз и реагирование на них
- ✓ Эмулятор атак

Политики защиты от угроз состоят из:

- ✓ ATP для SharePoint, OneDrive, Microsoft Teams и Office ProPlus.
  Защита организации при совместной работе пользователей и совместном использовании файлов путем определения и блокировки вредоносных файлов на сайтах групп и в библиотеках документов.
- ✓ Защита от фишинга ATP.
  Обнаружение попыток олицетворения пользователей и личных доменов. Применение модели машинного обучения и улучшенных алгоритмов обнаружения олицетворения для предотвращения фишинговых атак.

Преимущества Office 365 ATP план 2

- Лучшие средства анализа угроз и реагирования на них, позволяющие прогнозировать, изучать и предотвращать атаки злоумышленников.
- Трекеры угроз предоставляют новейшую аналитику касательно преобладающих проблем кибербезопасности. Например, можно просматривать сведения о новейших вредоносных программах и принимать контрмеры, прежде чем они станут реальной угрозой для организации.
- Отчет обозревателя угроз, также именуемого обозревателем (или обнаружение в режиме реального времени), — это отчет, получаемый в режиме реального времени, с помощью которого можно определить и проанализировать последние угрозы
- Эмулятор атак позволяет запускать реалистичные сценарии атак в организации для определения уязвимостей. Доступны имитации актуальных типов атак, в том числе целевой фишинг с целью сбора учетных данных, атаки с вложением, атаки путем распыления пароля, атаки методом подбора пароля.

Мы предлагаем ряд комплексных мер по повышению безопасности и обеспечению высокого уровень удаленного доступа:

1. Azure AD + NPS + MFA

Интегрировать сервер политики сети (NPS) с Azure MFA, чтобы применять двухфакторную проверку подлинности пользователей, подключающихся к VPN-серверу.

В итоге: чтобы получить доступ, пользователю необходимо предоставить свои имя пользователя и пароль, а также другие сведения, которыми он управляет (второй фактор).

2. Azure AD App Proxy + MFA

Azure AD App Proxy приложений проверяет пользователя и устройство перед предоставлением доступа только к приложению (можно также добавить мониторинг и контроль сеансов)

В итоге: выполнив единый вход в AAD и подтвердив подлинность вторым фактором (MFA), пользователи получают доступ к облачным и локальным приложениям через внешний URL-адрес или внутренний портал приложений.

3. Conditional Access

Conditional Access позволяет гибко разграничивать доступ к приложениям и сервисам.

Используйте политики для пользователей/групп и настройки условий доступа, чтобы обеспечить высокую безопасность инфраструктуры.

При попытке выполнения входа будет выполняться проверка соответствия условиям политики и разрешение доступа, запрет, требование MFA или вход только с использованием определенного приложения.

Условия доступа включают в себя:

- ✓ интеллектуальная оценка риска при авторизации в режиме реального времени;
- ✓ расположение, откуда выполняется авторизация;
- ✓ используемое клиентское приложение;
- ✓ платформа и тип используемого устройства.

Системный интегратор

+7 495 980 23 45
market@infosec.ru
www.infosec.ru

Сервисный центр

+7 495 981 92 22
+7 495 980 23 45 доб.06
support@itsoc.ru
www.itsoc.ru

Центр противодействия кибератакам IZ SOC

+7 495 980 23 45
izsoc@infosec.ru
www.izsoc.ru

Центр противодействия мошенничеству

antifraud@infosec.ru

Информзащита
Системный интегратор