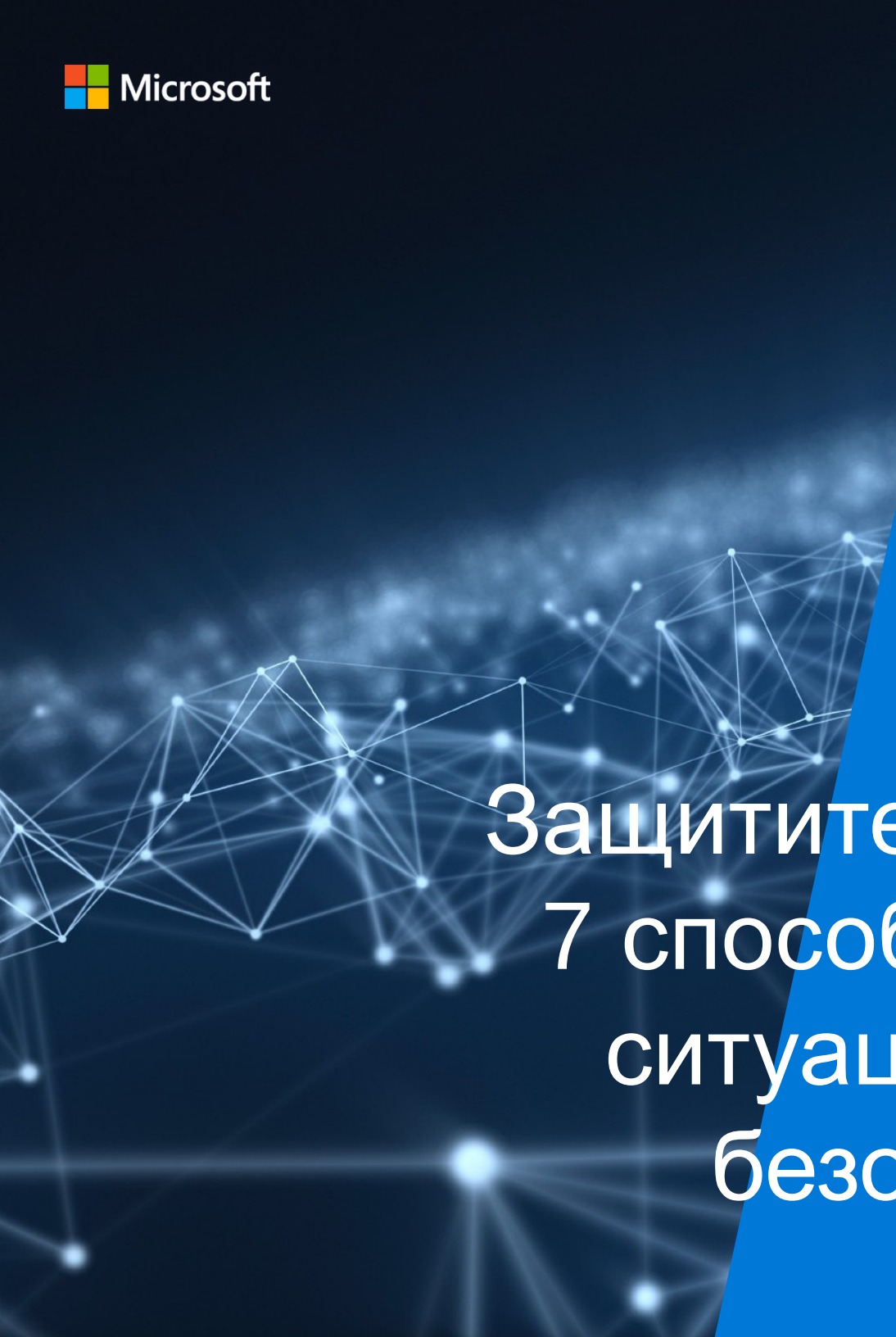
Microsoft



Защитите свои данные: 7 способов улучшить ситуацию в сфере безопасности

Корпоративная мобильность, обилие личных устройств, облако и предоставление приложений по модели «ПО как услуга» изменили способ ведения бизнеса и позволили предпринимателям и их сотрудникам стать более мобильными и эффективными в работе.

Однако переход к мобильным и облачным платформам стал причиной и других изменений — отказа от ограничений, связанных с географическим местоположением, более активного использования в работе общественных сетей (без домена) и личных мобильных устройств. Хотя эти изменения и повышают продуктивность, они могут подвергнуть конфиденциальные данные компании большему риску со стороны угроз безопасности, хакерских атак и взломов.

Можно ли предоставить сотрудникам все необходимое для эффективной мобильной работы и в то же время защитить данные? Можно.

В данной электронной книге мы обсуждаем семь областей, на которые компаниям следует обратить особое внимание для улучшения защиты данных и снижения риска кибератак.

«Защитите свои данные: семь способов улучшить ситуацию в сфере безопасности» — это первая электронная книга корпорации Майкрософт в серии, посвященной проблеме безопасности.

Семь способов улучшить ситуацию в сфере безопасности

- Уменьшить количество угроз, управляя удостоверениями и доступом.
- Управлять мобильными устройствами и приложениями.
- Применять политики условного доступа.
- Повысить защиту корпоративных данных.
- Предотвращать потери данных.
- Обеспечивать безопасную совместную работу.
- Уменьшить уязвимость перед вредоносным ПО.

Уменьшить количество угроз, управляя удостоверениями и доступом

Часто слабым звеном в безопасности компании становятся ее сотрудники, ведь они могут случайно раскрыть конфиденциальную информацию или указать данные рабочей учетной записи в социальных сетях. Отчасти это происходит потому, что управление приложениями в корпоративных ЦОД и общедоступных облачных платформах становится все более сложной задачей.

Сотрудники хотят иметь доступ к ресурсам и технологиям с различных устройств и не быть привязанными к одному месту работы. Такая повышенная мобильность может вызвать множество затруднений с точки зрения безопасности, например сложности управления доступом на основе пароля или местоположения.

Хакеры, атакующие компанию извне, ищут уязвимости в ее защите, например утечку учетных данных, для получения доступа к сетям и кражи информации о клиентах, интеллектуальной собственности или других конфиденциальных данных. Это может стать серьезной угрозой для вашего бизнеса, разрушить репутацию компании, нанести ей финансовый и л и правовой ущерб. Внутренние уязвимости не менее опасны. Так как же контролировать доступ к приложению, отслеживать кто, где, когда и зачем его использует?

Управление удостоверениями и доступом может помочь в снижении рисков.

- Избавьтесь от необходимости хранения нескольких учетных данных при помощи единой идентификации для доступа к облачным и локальным ресурсам.
- Ограничьте доступ сотрудников, оставив лишь те ресурсы, которые могут потребоваться им для работы.
- Отменяйте привилегии доступа при смене позиции сотрудника, его уходе из компании или если они больше не потребуются ему в работе.
- Используйте двухфакторную проверку подлинности при подозрительной активности.

- *Более 80 % сотрудников признались, что используют для работы несертифицированные приложения SaaS («ПО как услуга»)*[1]

[1] Источник: «Что скрывается за теневыми ИТ-ресурсами: шесть тенденций, влияющих на безопасность» («The hidden truth behind shadow IT – six trends impacting your security posture»), Frost & Sullivan

Подробнее

- *Управление удостоверениями и доступом*

Управлять мобильными устройствами и приложениями

С ростом использования в работе личных устройств (концепция BYOD) и приложений SaaS резко увеличились риски безопасности. Критически важные данные гораздо чаще попадают в общедоступное облако, которое уступает частному облаку и локальным решениям по уровню защиты. В подобной ситуации компаниям приходится быстрее адаптироваться, чтобы сохранять приемлемый уровень безопасности.

В случае кражи или потери устройства, а также если сотрудник оставил его без внимания, безопасность данных находится под угрозой. Использование корпоративных данных в личных приложениях также влечет за собой определенные риски. Так как же защитить данные в эпоху BYOD, но не в ущерб продуктивности сотрудников?

Начнем с основ:

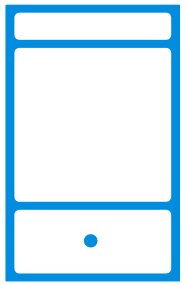
- Не меняйте процессы работы пользователей; создайте правила, которых они смогут легко придерживаться. Управляйте только важными приложениями, а не всем устройством.
- Расскажите сотрудникам об ИТ, которые используются для защиты устройств.
- Защищайте только корпоративные данные. Выберите решения, позволяющие сотрудникам свободно использовать устройства в личных целях.

- *Согласно оценкам около 52 % работников в сфере ИТ из 17 разных стран используют для работы более трех устройств[1].*

[1] Источник: «Использование личных устройств в работе становится причиной дополнительных угроз безопасности» («Employee devices bring added security concerns»), Синди Бейтс (Cindy Bates), блог для предприятий малого и среднего бизнеса, Майкрософт США

Подробнее

- *Microsoft Intune*



Применять политики условного доступа

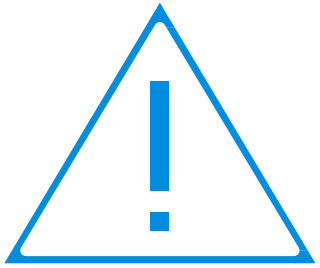
Условный доступ ограничивает доступ к корпоративным ресурсам в зависимости от удостоверения пользователя и состояния устройства. Он также применяет политики на основе местонахождения и уровня конфиденциальности данных приложения. Например, чтобы получить доступ к приложению управления отношениями с клиентами (CRM) из кафе, потребуется многофакторная проверка подлинности. Причиной тому являются местонахождение пользователя и высокий уровень конфиденциальности данных системы CRM. Другой пример — электронная почта. Чтобы получить доступ к корпоративной электронной почте, устройство должно соответствовать определенным политикам (например, поддерживать шифрование и защиту при помощи ПИН-кода). Обеспечив правильное применение политик условного доступа, компания сможет улучшить общую ситуацию в сфере безопасности.

Какими станут первые шаги в этом направлении?

- Определите, какая политика доступа к мобильным устройствам подойдет вам и вашему бизнесу. Например, можно управлять всем устройством или только критически важными приложениями, такими как Outlook, для доступа к корпоративной почте.
- Используйте динамические группы, чтобы предоставить пользователям доступ к необходимым приложениям в зависимости от их ролей.
- Организуйте многофакторную проверку подлинности. Пользователи будут проходить аутентификацию в два этапа, а значит, у системы появится дополнительный уровень защиты. Первый этап — традиционная комбинация имени пользователя и пароля. Второй — зачастую включает физический компонент, который виртуально смоделировать невозможно. Например, использование карточки с ключом и ввод ПИН-кода, вход на веб-сайт с использованием одноразового пароля, вход через клиент VPN с цифровым сертификатом или сканирование отпечатка пальца.

Подробнее

- *Условный доступ Azure Active Directory*
- *Общие сведения об условном доступе*
- *Условный доступ с Microsoft Intune*
- *Office 365 с Microsoft Intune*
- *Windows 10*



Повысить защиту корпоративных данных

Возможности мобильной работы могут значительно увеличить продуктивность сотрудников и частоту доступа к рабочим ресурсам, однако они также повышают риск случайной утечки данных через приложения и сервисы (например, электронную почту, социальные сети и облако). Предоставление работникам безопасной среды для удаленной работы — ключевой фактор для обеспечения безопасности и сохранения высокого уровня продуктивности. К примеру, работник может отправить новые чертежи с личной электронной почты, скопировать информацию в социальные сети или сохранить рабочую информацию в личное облачное хранилище. Так как же разрешить использование личных устройств в работе и при этом сохранить конфиденциальные данные в безопасности?

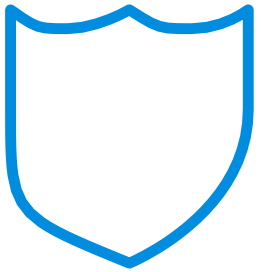
Защита корпоративных данных (WIP) помогает уберечь данные от потенциальной утечки в нежелательные приложения и хранилища, не нарушая работы пользователя с этой информацией.

Приступая к работе:

- Убедитесь, что устройства полностью зашифрованы на случай пропажи или хищения.
- Активируйте WIP в своей корпоративной среде, что позволит управлять приложениями и данными, исключая нежелательные изменения.

Дополнительная информация

- *Защита корпоративных данных (Windows 10)*
- *Общие сведения о BitLocker*
- *Microsoft Intune*



Предотвращать потери данных

Возможность получить общий доступ к документам при помощи электронной почты и других онлайн-инструментов является важным аспектом для повышения продуктивности сотрудников, однако влечет за собой определенные риски, связанные с человеческим фактором. Сотрудники могут случайно отправить важные данные получателю, которому они не предназначались, или приложить к письму не тот документ, непреднамеренно раскрыв конфиденциальную информацию. Поэтому специалисты по безопасности должны четко понимать все риски и преимущества совместного использования данных, а также разрабатывать соответствующие стратегии, чтобы минимизировать потери данных и обеспечить более высокий уровень защиты. Возникает вопрос: как обезопасить конфиденциальную информацию, не отказываясь от общего доступа к файлам в электронной почте?

Для начала сократите вероятность утечки.

- Узнайте больше о возможностях защиты от потери данных (DLP) в вашей экосистеме, чтобы гарантировать безопасность конфиденциальной информации в процессе хранения, перемещения или совместного использования. Например, можно ограничить использование электронной почты до переписки внутри организации или назначить пользователям цифровые права, определяющие, какие письма будут им доступны.
- DLP можно применять и за пределами электронной почты. Некоторые программы для обработки текстов, таблиц и презентаций также поддерживают настройки доступа для предотвращения несанкционированного использования файлов.

Дополнительная информация

- *Office 365 защита от потери данных (DLP)*
- *Microsoft Office 365*

Обеспечивать безопасную совместную работу

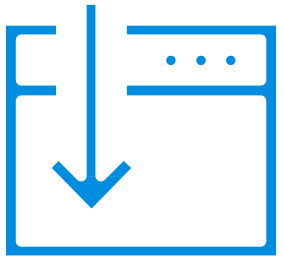
Что касается совместного использования информации, порой удобство оказывается важнее соблюдения всех требований защиты, что сильно усложняет работу специалистов по безопасности. Выбирая способы делиться информацией, сотрудники могут быть весьма изобретательными, тем самым ставя под угрозу сохранение конфиденциальности данных и рискуя потерять важные сведения. Как предоставить им все необходимое для совместной работы, при этом снизив риск утечки информации?

Предложите сотрудникам надежное гибкое и простое в использовании решение, соответствующее их требованиям.

- Позаботьтесь о наличии надежных инструментов для совместного использования информации и распределении прав доступа среди сотрудников. Сюда входит безопасное решение для совместного использования документов (например, SharePoint), сетевая папка или облачное хранилище с ограниченным доступом.
- Организуйте поддержку управления цифровыми правами или другой защиты электронной почты, чтобы обезопасить отправку конфиденциальных данных.
- Обеспечьте простой и безопасный общий доступ к информации для внешнего и внутреннего взаимодействия.

Подробнее

- *Управление правами Azure*
- *Совместное использование защищенных файлов*
- *Отправка зашифрованных сообщений электронной почты*
- *Microsoft Office 365*
- *SharePoint*
- *Microsoft Azure*



Уменьшить уязвимость перед вредоносным ПО

Заражение вредоносным ПО зачастую происходит по ошибке пользователя. Схемы фишинга и подмен стали намного сложнее. Теперь мошенники обманывают пользователей, отправляя им фальшивые электронные письма якобы от лица известных брендов, заманивая их ложными новостями и предлагая загрузить вредоносные файлы под видом безобидных предложений. Нельзя запретить работникам пользоваться Интернетом, социальными сетями или личной электронной почтой на их собственных устройствах. Но как помочь им делать это в более безопасном режиме?

Первый шаг к безопасности — обучение.

- Попросите сотрудников ознакомиться с основным руководством или пройти полный курс обучения, в котором говорится о стандартных случаях заражения вредоносным ПО.
- Научите пользователей внимательно проверять ссылки, чтобы удостовериться в их надежности. Рассмотрите возможность внедрения решений по защите электронной почты, чтобы предотвратить заражение вредоносным ПО или фишинг через почту сотрудников.
- Предложите сотрудникам не использовать приложения, загруженные из ненадежных источников.

Подробнее

- *Windows 10*
- *Защитник Windows*
- *Windows Device Guard*
- *Microsoft Office 365*

Уделите особое внимание этим семи областям, чтобы повысить безопасность вашей организации

Позволить сотрудникам быть мобильными не значит подвергнуть ваши корпоративные данные риску. Благодаря тщательному планированию, правильно подобранным инструментам и обучению вы можете предоставить сотрудникам возможность работать в любое время в любом месте, не подвергая конфиденциальность данных серьезной угрозе.

Узнайте больше о кибербезопасности