Microsoft

It's only natural

Intelligent security

Говорим на одном языке: кибербезопасность для бизнеса

Введение

В последние годы информационная безопасность является одной из наиболее обсуждаемых тем в ИТ.

Возросшее число хакерских и вирусных атак, громкие истории компрометации данных создают резонанс в мире информационных технологий.

Зачастую руководитель компании малого или среднего бизнеса не имеет глубокого представления об информационной безопасности, рисках, современных угрозах и не желает вникать в тонкости ИТ. Чаще всего у него есть представление о двух или трех угрозах, которые в общем виде беспокоят лично его. Согласовывая бюджет, руководителю важно, чтобы инвестиции в новое ПО были оптимальны в плане затрат и обеспечивали положительный для бизнеса эффект.

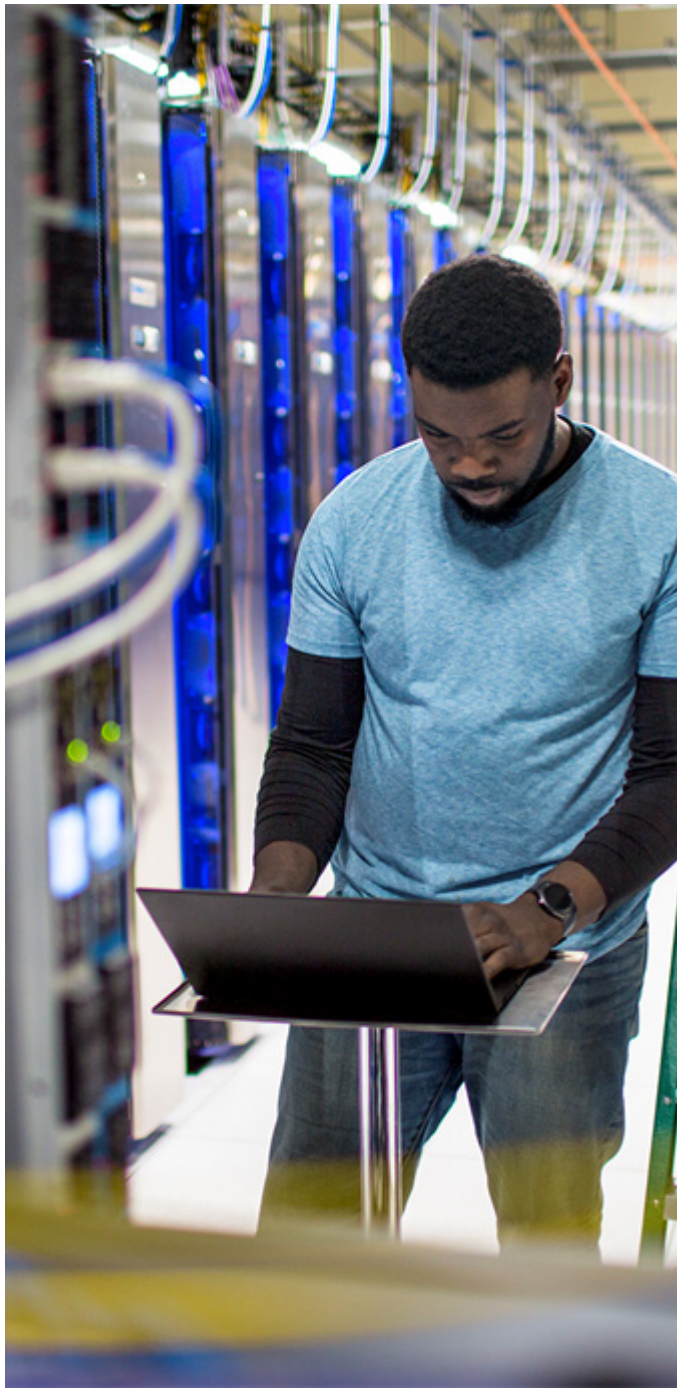
Данное пособие поможет Вам подобрать аргументы для разговора с человеком, принимающим решение, на его языке – языке бизнеса. В брошюре рассказывается, как решения Microsoft (Microsoft 365 и Microsoft Azure) позволяют снизить риски угроз для бизнеса и, возможно, предотвратить катастрофу, связанную с хакерской или вирусной атакой.

Как работать с пособием

В тексте вы найдете примеры различного рода атак и защиты от них. Описание дано как техническим языком, так и языком, понятным лицам, которые принимают решения по внедрению.

Подход к беседе об информационной безопасности

Беседа об информационной безопасности с лицами, принимающими решения, имеет свои особенности. Людям не свойственно уделять внимание безопасности до тех пор, пока «все хорошо». Компании, которые столкнулись со значительной потерей данных из-за действий вирусов-шифровальщиков, значительно больше уделяют внимания безопасности, чем те, кто ещё не сталкивался с этим. С другой стороны, безопасность не может быть 100%. До тех пор, пока система работает, она подвержена опасности. Наша задача – показать наличие рисков и уменьшить их до приемлемого уровня. Поскольку снижение рисков опирается на приобретение программного обеспечения, важно понимать, что выгоднее платить за безопасность, чем расплачиваться за её отсутствие.



Основные проблемы в сфере информационной безопасности в малом и среднем бизнесе

1 **Люди** – самое слабое звено. Они зачастую не знают ценности информации с которой работают и достаточно беспечны в её защите.

2 **Доступность инструментов.** На сегодняшний день порог входа в «хакинг» достаточно низкий. Разработаны и доступны тысячи инструментов, которые может бесплатно скачать любой начинающий специалист. По этой причине количество условных «хакеров» в наши дни достаточно велико. Такие «хакеры» вряд ли смогут взломать хорошо защищенную инфраструктуру, но компании, которые не заботятся об информационной безопасности, попадают в группу риска.

3 **«Наша компания слишком маленькая, кому мы нужны?»** Существует такое распространённое мнение среди компаний малого и среднего бизнеса. Даже небольшая компания может стать объектом целенаправленной атаки, но ещё большая проблема в том, что атакующие не выбирают цель. Атаки автоматизированы и атакуют все, что можно атаковать. После того, как атака будет выполнена успешно, атакующий будет проверять как можно использовать полученную информацию. В практике известны случаи, когда со скомпрометированного сервера компании хакеры пытались взламывать сервера государственных органов. Компании обнаруживали, что их взломали тогда, когда к ним приезжали спецслужбы для бесед и изъятия оборудования.

4 **Устаревшие технологии.** Проблема устаревших технологий заключается в том, что при создании в них проектировалась защита от угроз, которые были актуальны на момент создания ПО. Чем больше времени существует ПО «как есть», тем больше появляется атак, защиты от которых данное ПО не предусматривает. Не все атаки можно предотвратить с помощью «заплаток».

5 **Отсутствие специалистов по ИБ и недостаток ресурсов** для обеспечения безопасности у ИТ-специалистов. В малом и среднем бизнесе не всегда есть специалисты по информационной безопасности. Функции ИБ выполняются специалистом ИТ, а у него часто не остается достаточно времени на это, если системы приходится настраивать и поддерживать самостоятельно. Проблема в том, что функции ИТ заключаются в предоставлении работающей ИТ-услуги, а безопасность может усложнять её предоставление. Например, тщательно настроенный межсетевой экран может блокировать работу легитимных приложений. У ИТ-специалиста есть выбор: мониторить используемые порты приложением или выключить межсетевой экран. Второй вариант быстрее дает результат, поэтому некоторые выбирают его.

Угроза Пароль к электронной почте можно подобрать, спросить или получить из памяти веб-браузера

Решение

Office 365: Многофакторная аутентификация

Настройка двухфакторной проверки подлинности для Office 365

Языком ИТ

Вы наверняка знаете, что многие пользователи воспринимают свой пароль не как способ защиты от несанкционированного доступа, а как «прихоть администратора». Они весьма легкомысленно обращаются с паролями, при этом требуют ответственности за сохранность информации от ИТ департамента.

Многофакторная аутентификация требует не только знания пароля, но и ответственности пользователя за свое персональное устройство.

Многофакторная аутентификация легко настраивается для онлайн-сервисов и решает ряд проблем с безопасностью. Возможен телефонный звонок, смс, подтверждение в мобильном приложении или ввод цифр из мобильного приложения. Возможна гибкая настройка исключений. Например, не требовать второй фактор при работе с IP-адреса компании, но требовать при работе из дома. Возможно подключение к локальным сервисам. Например, доступ к терминальной сессии после ввода нескольких факторов.

Нарушение безопасности не исключается на 100%, но значительно затрудняется, поскольку злоумышленнику, помимо знания пароля, потребуется персональное устройство пользователя, а они с ними неохотно расстаются.

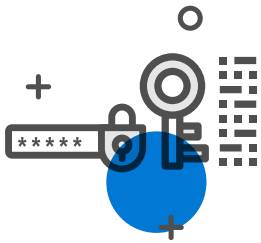
Заручитесь поддержкой руководства, иначе многофакторная аутентификация будет восприниматься как очередные «козни администратора».

Языком бизнеса

Одного только пароля уже недостаточно. Люди клеят стикеры с паролями, записывают их в файлах, сообщают друг другу, сохраняют в браузерах. Зачастую пароли очень простые – так удобнее. А ещё эти же логины и пароли используют для регистрации на различных сайтах и форумах с сомнительными настройками безопасности.

Когда вы подключаетесь к своему интернет-банку, помимо пароля, вам нужно указать код из смс. Почему рабочие документы должны быть меньше защищены?

Объясните сотрудникам, что лишние 15 секунд на ввод текста это адекватная цена за сохранность доступа к важной информации.



Угроза Вредоносные вложения электронной почты

Решение

Office 365: Б езопасные вложения ATP (Advanced Threat Protection)

Описание и настройка Office 365 Безопасные вложения ATP

Языком ИТ

Безопасные вложения — это возможность Microsoft 365 ATP, которая открывает каждое вложение в специальном гипервизоре. Проверяет вложение на вредоносность и принимает меры обнаружения угроз. Данная возможность защищает электронную почту даже до появления соответствующих сигнатур для антивируса.

Безопасные вложения ATP анализирует содержимое вложений наиболее известных типов файлов, таких как Word, PowerPoint, Excel, PDF, исполняемые файлы и файлы Flash.

Вложения тестируются в виртуальной среде с различными версиями операционных систем и приложений. Содержимое вложений выполняется под наблюдением искусственного интеллекта для обнаружения вредоносного поведения. Если вложение пытается инсталлировать трояна, шифровать файлы, передать управление на командный центр и т. д., то данное вложение определяется как вредоносное.

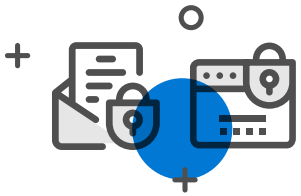
Администратор может получать копии исходных писем.

Языком бизнеса

Представьте две ситуации – вы открыли документы из вложения электронной почты и он:

1) Просто открылся
2) Запустил процесс, который передает данные с вашего ноутбука или шифрует другие документы

Внешне оба документа могут быть идентичными, но у них разное поведение. Электронная почта от Microsoft тестирует поведение документов до того, как письмо попадет в почтовый ящик. Если поведение похоже на п2, то письмо будет доставлено без вложения. Ни один шифровальщик не проникнет через корпоративную электронную почту. Система, в отличие от сотрудников, не поверит привлекательным письмам и сразу их удалит.

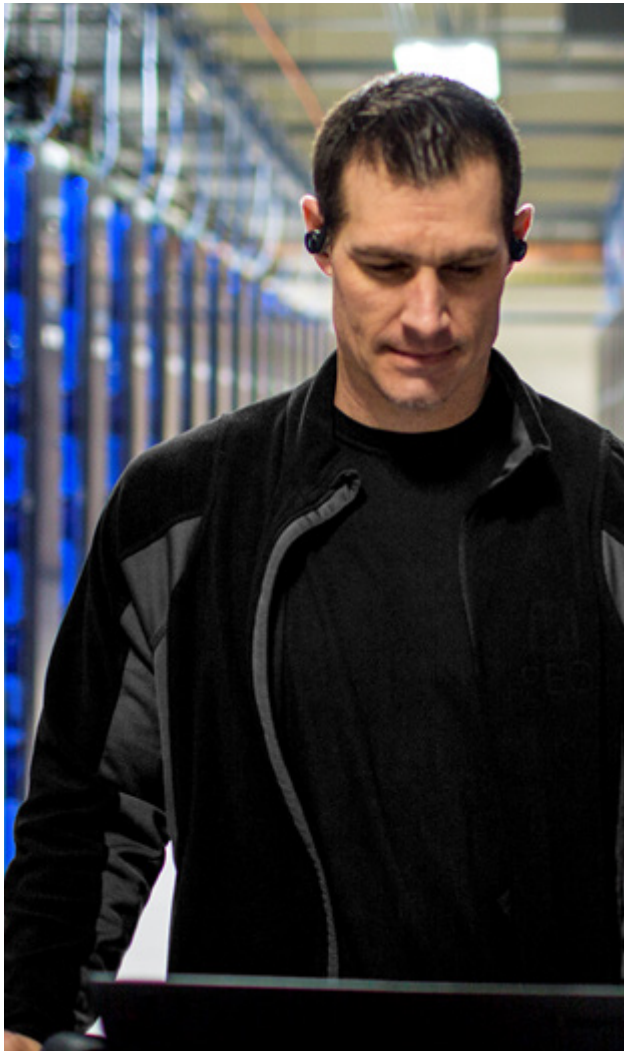


Угроза Вредоносные ссылки в электронной почте

Решение

Office 365: Безопасные ссылки ATP (Advanced Threat Protection)

Описание и настройка Office 365 Безопасные ссылки ATP



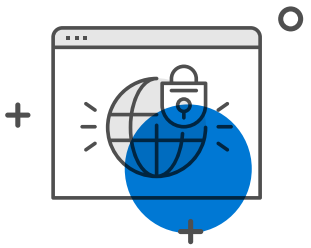
Языком ИТ

Безопасные ссылки – это возможность Microsoft 365 ATP, которая защищает пользователей от вредоносных ссылок, часто используемых в целях фишинга для сбора важной информации у пользователя. Когда сообщение со встроенной ссылкой доставляется получателю, страница или документ по ссылке могут быть безопасными на момент доставки, но небезопасными в момент клика по ссылке. Безопасные ссылки защищает пользователя, перезаписывая ссылку.

Когда пользователь кликает по ссылке в письме или документе, его запрос перенаправляется на сервер в среде Microsoft 365 для проверки URL по списку сомнительных сайтов. Если ресурс безопасен, то браузер перенаправляется на запрашиваемый сайт.

Если сайт в черном списке, переход блокируется и браузер отображает страницу с предупреждением. Блокируются переходы только по вредоносным ссылкам. Если в одном письме несколько ссылок, только вредоносные переходы будут заблокированы.

Администратор может вручную добавлять сайты в списки вредоносных.



Языкома бизнеса

В наше время те, кого мы называем «хакеры», давно стали маркетологами. Они рассылают привлекательные письма, создают похожие на настоящие копии сайтов банков и воздействуют на человеческие эмоции. Переход по ссылке из письма может закончиться вирусной эпидемией или потерей доступа к банку, площадке для торгов и т.д.

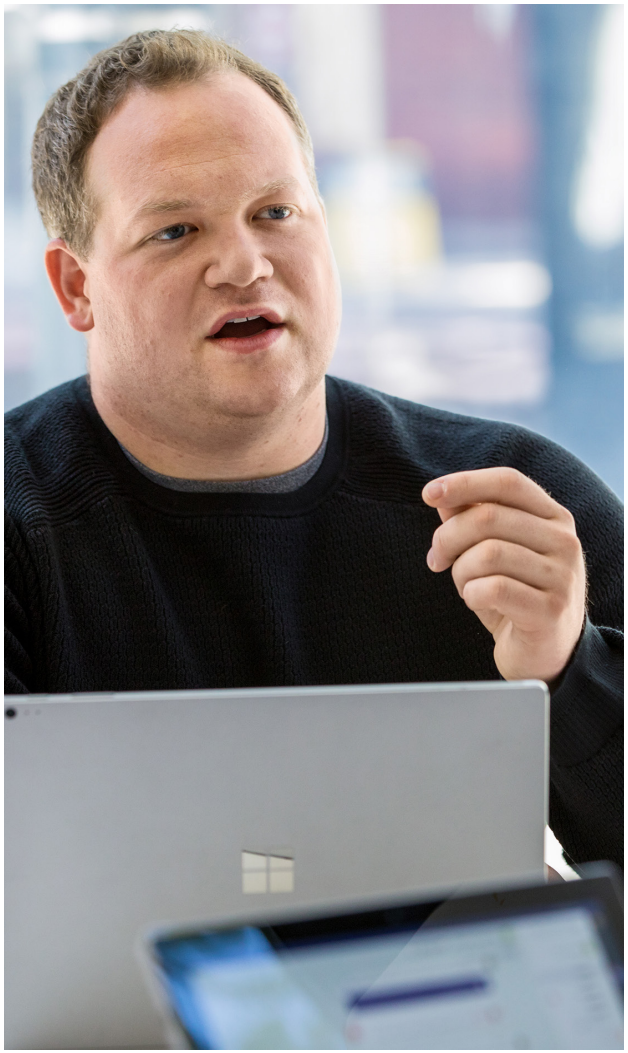
Информация о подобных ссылках попадает в Microsoft в течение нескольких минут. Попытки открыть ссылки на сайты с вирусами или сайты, выдающие себя за интернет-банки, будут заблокированы.

Угроза Атаки вирусов-шифровальщиков

Решение

Windows 10: Controlled Folder Access

Настройка возможности Контролируемый доступ к папкам



Языком ИТ

Возможность Controlled Folder Access позволяет запретить запись не доверенным процессам в указанные вами папки.

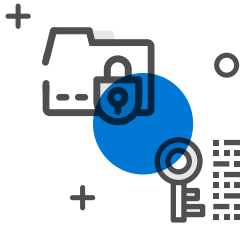
В случае проникновения шифровальщика Windows заблокирует любые попытки изменения файлов в защищенных папках, соответственно, важные файлы останутся нетронутыми. ОС придется переустановить, но данные сохранятся.

Полный список процессов не публикуется, но такие приложения как Powershell или cmd доверенными не являются, поскольку могут запускать вредоносные скрипты. Процессы типа Windows Explorer или MS Word не будут затронуты, но если вам нужно добавить неизвестный процесс в «белый список», такая возможность существует. Функция Controlled Folder Access опирается на антивирус Windows Defender и не работает при установленном стороннем антивирусе.

Языком бизнеса

Шифровальщики представляют серьезную проблему и нередко обходят антивирусную защиту. Даже если система была зашифрована, файлы в защищенных папках останутся нетронутыми.

Даже если антивирус опять не справится с вирусом-шифровальщиком, ваши документы останутся в полной сохранности.



Угроза Атаки вирусов-шифровальщиков

Решение

Attack Surface Reduction

Настройка возможности Уменьшение поверхности атак

Языком ИТ

Представляет из себя набор правил, включение которых позволит уменьшить вероятность взлома или заражения.

Примеры правил:

Блокировка исполняемого содержимого в клиенте электронной почты и веб-почте. Даже если пользователь скачал вредоносный код с личной почты, он не сможет его выполнить.

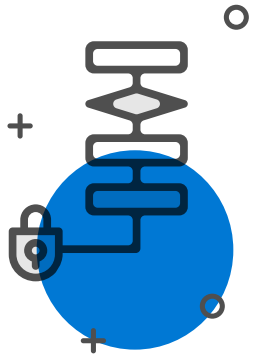
Блокировка создания дочерних процессов приложениями Office. Достаточно часто заражение начинается из-за вредоносных макросов в файлах Office. Это правило позволит запретить макросам вызывать сторонние приложения (например, Powershell или cmd), но и не будет мешать выполнению легитимных макросов, выполняющих, например, расчеты в Excel.

Блокировка создания дочерних процессов для Adobe Reader. Аналогичное правило для Adobe Reader.

Блокировка запуска приложений с USB-носителей. Название говорит само за себя.

И т.д.

Список правил пополняется с каждой новой сборкой Windows 10. Может работать в режиме аудита. Без блокировки, но с записью в журнал событий. Функция Attack Surface Reduction опирается на антивирус Windows Defender и не работает при установленном стороннем антивирусе.



Угроза Атаки вирусов-шифровальщиков

Решение

Network Protection

Настройка возможности Защита сети

Языком ИТ

В любой сети, сервере или рабочей станции есть брандмауэр. Даже если он корректно настроен, чаще всего он блокирует входящие соединения и разрешает практически любые исходящие.

Какие это несет угрозы:

- Пользователь может запустить ПО, которое передаст управление рабочей станцией на командный центр.
- У хакера появится полный доступ к рабочей станции и, как следствие, к внутренней сети компании.
- Пользователь может запустить ПО, которое будет отправлять данные на вредоносные адреса.
- Пользователь может кликнуть по ссылке и попасть на вредоносный сайт И т.д.

Функция Network Protection проверяет каждое исходящие соединение с базой знаний Microsoft. Если адрес успел засветиться где-то и помечен как вредоносный, соединение немедленно будет заблокировано. Функция Network Protection работает не только с конкретным веб-браузером, но и с любым приложением, использующим протоколы http/https. Может работать в режиме аудита. Без блокировки, но с записью в журнал событий. Функция Network Protection опирается на антивирус Windows De-fender и не работает при установленном стороннем антивирусе.

Угроза Атаки вирусов-шифровальщиков

Решение

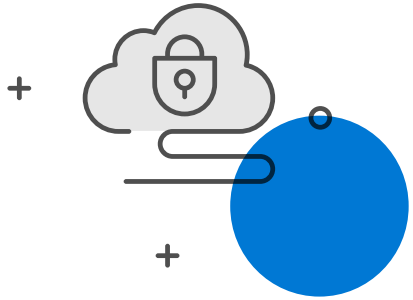
Office 365: OneDrive for Business

Настройка OneDrive для бизнеса в Windows 10

Языком ИТ

Если шифровальщики проникают в систему, они не только шифруют документы, но и архивы, а также удаляют теневые копии.
Настройте в Windows 10 синхронизацию документов в облачное хранилище OneDrive for Business и сможете все вернуть. Файлы будут синхронизироваться сразу после сохранения в специальном каталоге.
Клиент для синхронизации встроен в Windows 10, либо дополнительно устанавливается в Windows 7.

Минимальный доступный объем для хранения это 1ТБ на каждого пользователя.
Встроенная версионность позволит восстановить не только текущую версию файла, но и его предыдущие копии.



Языком бизнеса

Приходилось хвататься за голову из-за случайно удаленного документа или атаки вируса-шифровальщика? Или удалить фрагмент документа без возможности вернуть?

Помимо шифровальщиков есть пользователи, преднамеренно или нет удаляющие важные данные.

Работу системы можно настроить таким образом, что ваши документы на диске компьютера или ноутбука будут автоматически синхронизироваться с надежным хранилищем. При этом процесс работы с файлами и папками будет выглядеть как обычно.

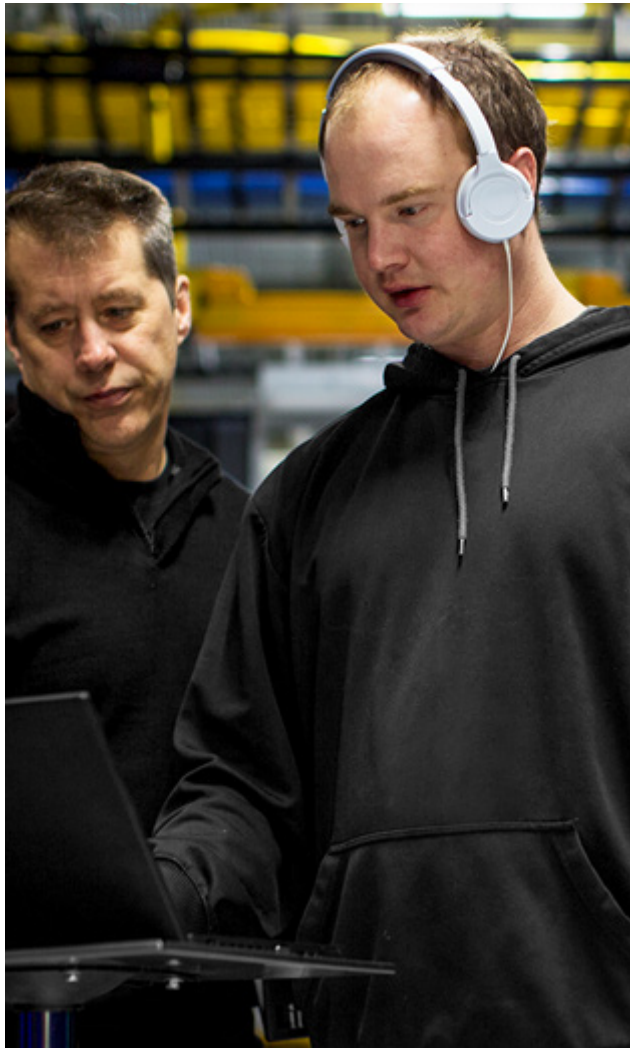
В тех случаях, когда файлы были зашифрованы, удалены или изменены, можно будет восстановить предыдущие версии. Все они сохраняются, сколько бы изменений в них не сделали. Это позволит вернуть предыдущую копию, которая не была зашифрована вирусом или утеряна по другой причине.

Угроза Скачивание информации с диска без пароля

Решение

Windows 10: Шифрование Bitlocker

Документация по Bitlocker



Языком ИТ

Вы прекрасно знаете, что можно извлечь жесткий диск и подключить его к другому ПК. Или загрузиться с DVD-диска и получить доступ к файловой системе. Ни в одном, ни в другом случае не требуется знать пароль от входа в систему.
И, конечно, существуют еще съемные носители, которые легко потерять. При этом стоимость информации на них зачастую многократно превышает стоимость носителя.

В связи с этим необходимо шифровать диски. Однако, как и любая мера для обеспечения безопасности, это добавляет некоторые неудобства и риски.
Правильная настройка Bitlocker минимизирует эти риски. Ключи восстановления можно хранить в Active Directory, а в случае физической порчи диска данные можно будет восстановить. Для большей надежности рекомендуется выполнять архивацию данных.

Языком бизнеса

В наше время потерять информацию проще всего вместе с устройством.

Ноутбук, который был забыт в аэропорту на досмотре, флешка, выпавшая из сумки. Все это не только расходы на приобретение нового устройства, но и серьезные риски несанкционированного доступа к информации.

Даже если ваш ноутбук защищен паролем, это не помешает ИТ-специалисту извлечь оттуда информацию. Нередко в таких ноутбуках можно найти документы со списком паролей или сохраненные пароли в браузере.

Зашифруйте диски и флешки с важными данными. Пропажа или изъятие устройства по-прежнему будет досадной, но к данным никто не получит доступа.

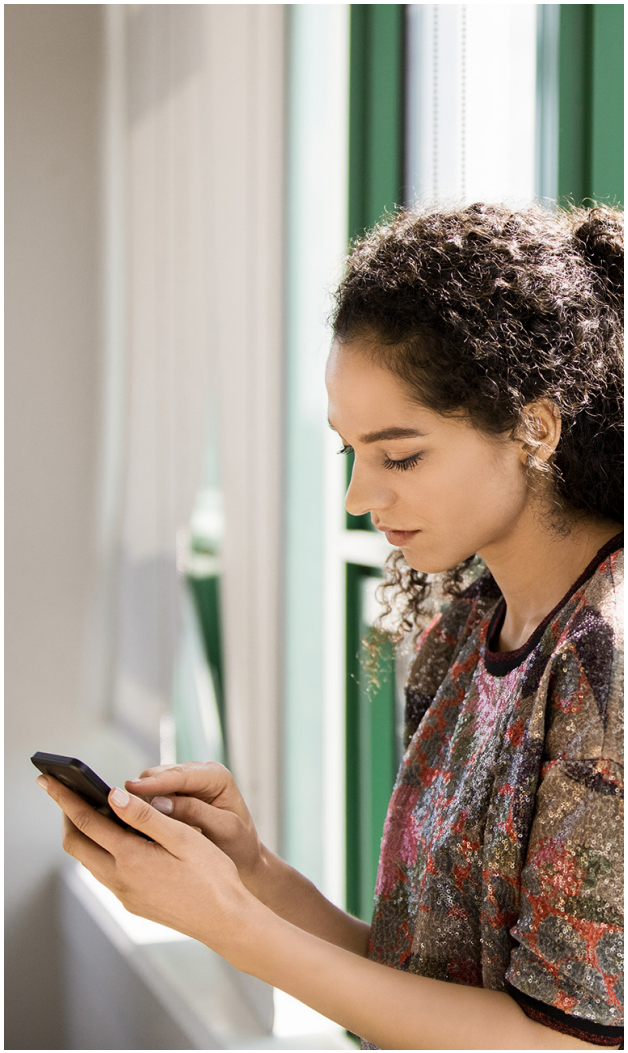
Данные будут надежно зашифрованы и недоступны для любопытных пользователей, нашедших ваше устройство.

Угроза Скачивание информации с диска без пароля

Решение

Microsoft Intune

[Документация по Microsoft Intune](#)



Языком ИТ

Microsoft Intune — это MDM система, управляющая устройствами из облака, которая позволяет выполнить управление приложениями независимо от местоположения пользователя.

Управление доступно для ряда устройств: iOS, Mac OS X, Android, Windows 8.1 и Windows 10.

Основные возможности:

• Доступ к электронной почте и документам только с настроенных компанией устройств.
• Настройки безопасности: пинкод, проверка на наличие root/jailbreak, запрет установки приложений не из магазина и т.д
• Полное или частичное удаление данных с устройства
• Развертывание сетей Wi-Fi, сертификатов
• Развертывание приложений, срздание ограничений внутри приложений. Например, запрет копирования текста из Outlook.

Вы не можете заставить пользователей подключить своё устройство к MDM, но вы можете запретить им получать доступ к ресурсам компании с неуправляемых устройств. Поскольку пользователям нужен доступ к ресурсам, им придется подключить свои устройства для управления.

Языком бизнеса

Компания, занимающаяся исследованиями в области информационной безопасности, проводила следующий эксперимент: в общественных местах США и Канады были «случайно забыты» мобильные телефоны. В телефонах было установлено ПО, отслеживающее все действия с устройством. 60% нашедших не пытались вернуть устройство. В течение 1-2 часов новый владелец начинал просматривать документы, фотографии и открывал приложения.

Основная угроза, связанная с мобильными устройствами, следующая - устройства личные, а информация на них может быть и корпоративной. Возможности управлять личными устройствами весьма ограничены.

Пользователи достаточно беспечны с личными устройствами: они не шифрованы, часто не имеют пинкода, на устройства устанавливаются сомнительные приложения, а само устройство может быть потеряно. Также уволенный сотрудник может сохранить архив почты или контакты клиентов в своем смартфоне.

Если сотрудники компании работают с корпоративной почтой или документами на мобильных устройствах, вы должны иметь возможность защитить данные, принадлежащие компании. Подключение мобильных телефонов к сервису Intune даст вам возможность настроить телефоны сотрудников более безопасно, а также удалить рабочие (или все) данные при увольнении сотрудника.

Вместе с уволенным сотрудником не «уйдут» корпоративная почта и рабочие документы на его личном смартфоне. А в случае кражи или потери устройства – данные можно удаленно стереть.

Угроза Вирусы

Решение

Windows 10: Windows Defender

Описание Windows Defender

Языком ИТ

Антивирус Microsoft Security Essentials, который использовался в предыдущих версиях, был достаточно простым. Windows Defender является правопреемником Security Essentials, но кардинально отличается от предшественника.

Основное преимущество — это интеграция с Windows 10 и улучшение механизма с каждой новой сборкой Windows 10.

Антивирус полностью бесплатный для корпоративного использования и может управляться групповыми политиками.

Некоторые функции, например получение централизованной отчетности, требуют коммерческих средств управления.

Языком бизнеса

Антивирус — это не панацея, поэтому безопасность нельзя пускать на самотек, но антивирус должен быть. Он есть, встроенный и бесплатный. Windows является наиболее распространенной, а значит и самой атакуемой операционной системой.

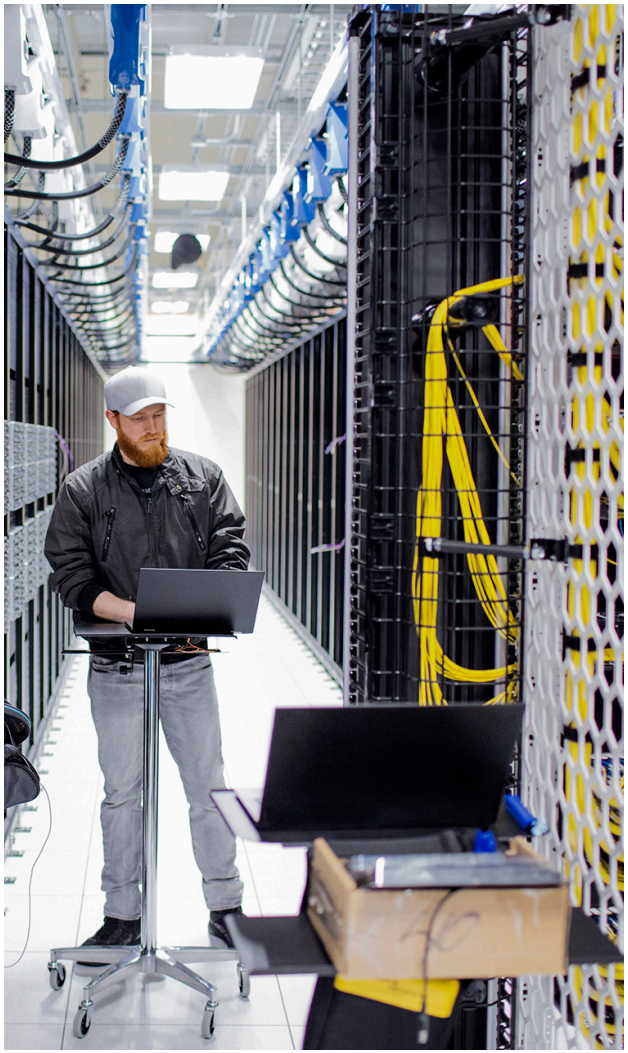
Те, кто зарабатывает деньги на взломах, ориентируются на наибольшую целевую аудиторию. Поэтому защита нужна встроенная, работающая с первой секунды. Windows 10 обладает этой встроенной защитой.

Угроза Утечка документов

Решение

Azure Information Protection

Документация по Azure Information Protection



Языком ИТ

Технология защиты документов путем их шифрования и назначения прав на доступ другим пользователям, позволяет сохранять заданные ограничения даже в случае утечки документов за пределы организации.

Azure Information Protection помогает сохранить конфиденциальную информацию внутри компании и позволит избежать утечек этих сведений.

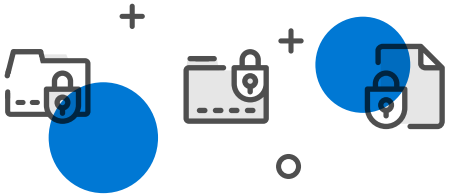
Технология интегрируется с приложениями Office, позволяя шифровать файлы из приложения Microsoft Word, а также из электронной почты Microsoft Exchange, предоставляя возможность применять её не только вручную, но и автоматически, по заданным правилам. Например, сотрудник отправляет письмо с вложением за пределы компании/на определенные адреса/ определенные файлы и т.д. Вложение может быть зашифровано автоматически.

Языком бизнеса

Даже если кто-то попытается вынести конфиденциальную информацию за пределы компании, то он просто не сможет открыть документ.

Если менеджер захочет отправить клиентскую базу конкурентам по почте, то такое письмо не сможет прочитать другая компания, как бы ни старалась.

И, наконец, можно установить ограничения на доступ к документам, чтобы никто лишний не увидел информацию, доступную только определенному кругу лиц.

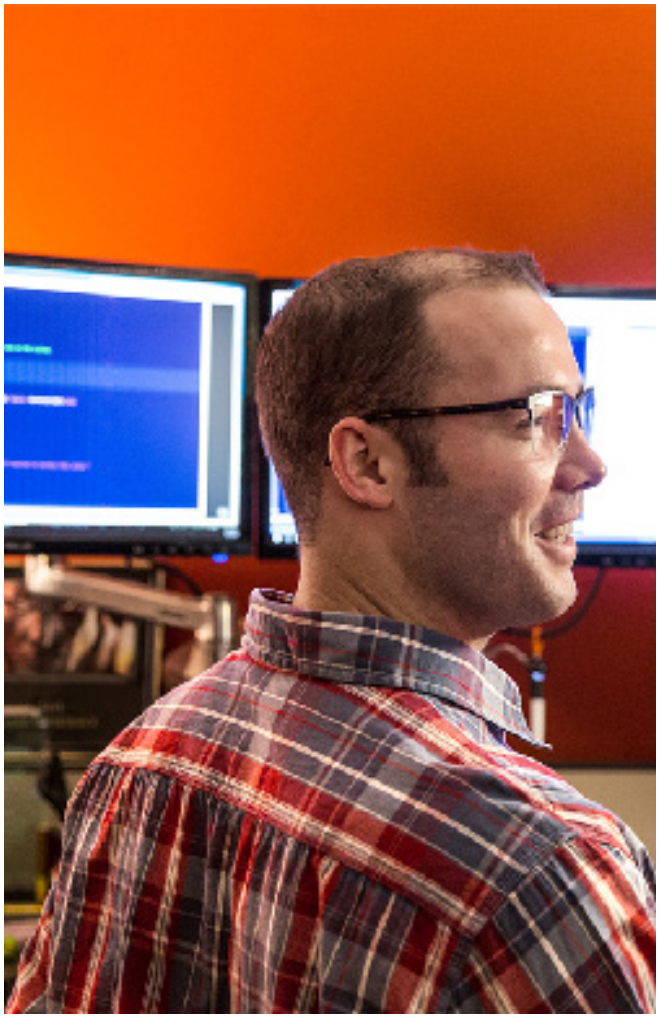


Угроза и еще утечка документов

Решение

Office 365 DLP (Data Loss Prevention)

Детальный обзор Office 365 DLP



Языком ИТ

Набор политик для Exchange Online, Share-point Online и OneDrive for Business для защиты конфиденциальной информации. Политика может запретить ряд действий с конфиденциальной информацией. Например, запретит пересылку за пределы компании или запретит скачивание на локальный ПК.

Администратор может быть уведомлен о попытках пользователей выполнить запрещенные действия.

Шаблон конфиденциальной информации, обнаруживающий данные российских паспортов, по умолчанию отсутствует в системе. Необходимо разработать самостоятельно или обратиться за помощью к системным интеграторам.

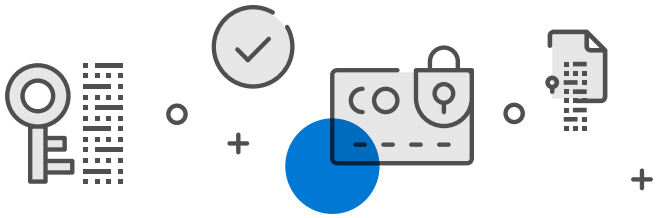
Языком бизнеса

Государство требует от компаний оберегать персональные данные от утечки.

Что делать, если сотрудник случайно отправил документ по электронной почте с паспортными данными?

Показательный случай: при подготовке Саммита G20 в Брисбене в 2015 году, сотрудник Австралийского департамента по иммиграции случайно отправил документ с паспортными данными лидеров стран G20 организаторам Азиатского кубка по футболу. Когда сотрудник вводил адрес коллеги в почте, автозаполнение подсказало адрес, а сотрудник его не проверил и отправил письмо.

Ваш администратор может настроить политику, блокирующую отправку писем, в которых обнаружены паспортные или другие персональные данные.



Угроза Физическая безопасность – риски проникновения

Решение

Использование дата-центра Microsoft

Языком ИТ

Безопасность инфраструктуры складывается из ряда факторов, в том числе безопасности физической. Когда оборудование находится на территории компании, организация физической безопасности может быть нетривиальной задачей.

Некоторые аспекты:

1) Серверную в офисе необходимо располагать правильным образом. В том числе стены серверной не должны примыкать к внешним стенам или иметь окна.

2) Необходима система поддержания в заданных пределах параметров температуры и влажности

3) На дверях должны быть электронные замки

4) В ЦОД должны быть фальшполы

5) В ЦОД должна быть система пожаротушения

6) Оборудование и системы хранения должны быть шифрованы

7) Должна быть обеспечена физическая безопасность здания в целом

Обо всем этом и не только уже позаботился Microsoft. С точки зрения безопасности, ваши данные будут значительно лучше защищены там, где есть все для этого необходимое.

Языком бизнеса

Когда все данные находятся рядом, так, конечно, спокойней. Но те, кто законно или незаконно смогут попасть на территорию компании, тоже смогут завладеть вашими данными. Для этого не нужно быть хакером, достаточно просто унести оборудование.

В Дата-центрах работают системы контроля доступа, пропускной режим, круглосуточное видеонаблюдение и охрана. А доступ третьих лиц затруднен или практически невозможен, особенно если дата-центр, где хранятся ваши данные, расположен в другой стране.

Небольшие компании, как правило, самостоятельно не могут позволить себе такой уровень безопасности, охрану серверов в офисе, контроль доступа и видеонаблюдение за серверами.

Угроза Физическая безопасность – риски проникновения

Решение

Использование дата-центра Microsoft

Языком ИТ

Давайте отправимся на виртуальную экскурсию в один из ЦОДов Microsoft.

Для начала его требуется найти. Адреса ЦОДов засекречены, посещение возможно только в определенных случаях (например, аудит) и с полным сопровождением сотрудниками безопасности. Даже если злоумышленник каким-то образом узнает адрес одного из ЦОДов, этой информации ему будет недостаточно. Ему также потребуется узнать в каком ЦОДе расположены именно ваши данные.

Все оборудование в контейнерах имеет жизненный цикл и регулярно меняется, не дожидаясь выхода из строя.

Чтобы попасть в ЦОД, потребуется пройти множество слоев безопасности: мультифакторная защита, биометрия, прохождение ряд помещений-man-trap'ов. Каждое перемещение фиксируется с помощью видеонаблюдения.

Попав, наконец-то, в ЦОД, вы увидите множество контейнеров с серверами, системами хранения и т. д. Ни аудиторы, ни сотрудники не знают в каком именно контейнере находятся ваши данные.

Все оборудование в контейнерах имеет жизненный цикл и регулярно меняется, не дожидаясь выхода из строя. По завершении жизненного цикла, системы хранения отправляются в шредер.

Оборудование находится под постоянным мониторингом во избежании инцидентов с производительностью и безопасностью.

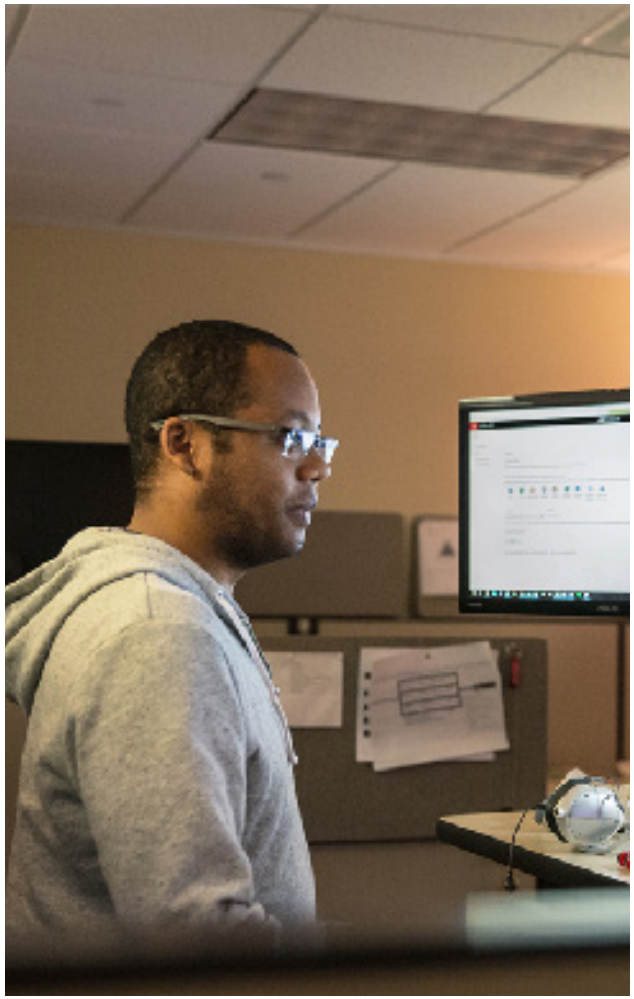
По завершении жизненного цикла, системы хранения отправляются в шреддер. Оборудование находится под постоянным мониторингом во избежание инцидентов с производительностью и безопасностью. ЦОДы обладают множеством сертификаций, полученных в результате аудита и подтверждающих надежность. Только несколько компаний в мире могут позволить себе такой уровень защищенности.

Угроза отсутствие архивации данных

Решение

Резервная копия в дата-центре

Документация по Azure Backup



Языком ИТ

Средство резервного копирования данных Microsoft Azure представляет собой базовое решение для архивации и восстановления данных, дополняющее существующие средства архивации.

Даже если локальный архив был потерян или испорчен, резервная копия в дата-центре Azure будет храниться столько, сколько пожелаете.

Архивация в облако является альтернативой работы с ленточными накопителями. Зачем используют ленты? Для недорого и надежного долговременного хранения. Но хранение лент не бывает недорогим и надежным одновременно. Невысокая стоимость носителей компенсируется расходами на транспортировку, аренду надежного помещения для хранения лент, учет и управление. Если пренебречь этими мерами, то носитель может быть уничтожен при любом инциденте.

Хранение в облаке дает сопоставимые ценовые характеристики при значительно более простом управлении и учете. Не требуется никуда ничего возить или искать нужную ленту на полках. Достаточно зайти на портал, поиском найти требуемый архив и нажать кнопку для восстановления.

Архивация работает на основе агентов. Если архивировать требуется только файлы, то достаточно инсталлировать агент на файловый сервер и запланировать операцию резервного копирования. Если требуется архивация виртуальных машин, баз данных или восстановление на пустое железо, инсталлируется специальный сервер Azure Backup Server, бесплатно предоставляемый компанией Microsoft и выполняющий резервирование централизованно.

Языком бизнеса

Локальное оборудование может выйти из строя, данные могут быть случайно или преднамеренно стерты. В таких случаях спасает резервная копия данных.

А что, если копия тоже была уничтожена? Это может произойти из-за пожара, ограбления или просто небрежного хранения носителей.

Однажды в американской киностудии, снимавшей известный мультфильм, произошел сбой, и большая часть отснятого материала была уничтожена, а архив не восстановился из-за небрежного хранения. Спасло мультфильм то, что один сотрудников накануне аварии скопировал отснятый материал и отвез домой, чтобы там поработать.

Организация надежного хранения архивов — это дорого. А даже правильное хранение может упираться в человеческий фактор.

Крупная больница в штате Юта хранила архивы с информацией о пациентах в защищенном хранилище. Ежедневно курьер забирал носители с данными и отвозил в хранилище. Однажды перед выходными курьер решил не отвозить носители в тот же день и оставил коробку в машине на ночь. Ночью машину ограбили и носители также были украдены, а компания заплатила миллионы долларов своим пациентами.

Хранение в облаке технологически надежно и лишено человеческих недостатков.

Годовой отчёт бухгалтера, база данных по зарплатам – теперь всё можно восстановить, даже если это было удалено преднамеренно или изъято.

Угроза если УЖЕ взломали

Решение

Advanced Threat Analytics (локально)

Azure Advanced Threat Protection (в облаке)

Документация по Advanced Threat Analytics

Языком ИТ

Ни одна защита не дает 100% гарантии. Проблема заключается в том, что компании обнаруживают взлом спустя несколько месяцев после непосредственного инцидента, когда все данные злоумышленником получены. Чтобы этого не допустить, требуется не только защищать, но и отслеживать.

Традиционно эту функцию выполняют системы IDS (Intrusion Detection System), а их современный аналог — это UBA (User Behavior Analysis).

Система UBA выполняет последовательное изучение ряда поведенческих признаков сотрудников: в какое время работает, на какие устройства логинится, к каким файлам получает доступ, в каких группах состоит и т. д. После построения поведенческого профиля пользователя система будет сообщать об аномалиях в поведении. Такие аномалии могут быть замечены как за сотрудником-инсайдером, так и злоумышленником, скомпрометировавшим учетную запись пользователя.

Система UBA может быть реализована двумя способами:

• Инсталлируется локально и анализирует траффик Active Directory. Называется Microsoft ATA • Расположена в облаке, локально инсталлируются агенты на контроллеры домена. Называется Azure ATP

Языком бизнеса

Ни одна защита не дает 100% гарантии.
Особенно сложно защищаться от тех, кому уже доверяют: сотрудников. Никто не гарантирует, что лишенный премии сотрудник не совершит диверсию или скопирует данные. Система анализа поведения сотрудников поможет обнаружить нетипичное поведение.

Если сотрудник задержался после работы, чтобы распечатать конфиденциальные данные, система об этом сообщит.

Или, например, в случае если сотрудник пытается получить доступ к документам, которые обычно не требуются ему для выполнения своих рабочих обязанностей.

Заключение

Исходя из количества описанных угроз и способов защиты можно сделать вывод, что безопасность — это комплексный подход. Не существует одной волшебной кнопки, нажав на которую все станет защищенным. Как и не существует одного программного продукта, обеспечивающего безопасность на всех уровнях. Для удобства и экономии компания Microsoft предлагает свои программные продукты не только в виде отдельных компонентов, но и в наборах. Набор, включающий в себя большинство описанных возможностей, называется Microsoft 365. Ознакомиться с предложениями Microsoft 365 можно на его официальной странице https://www.microsoft.com/ru-ru/microsoft-365

Для ИТ-специалистов доступен курс обучения по Microsoft 365: https://p.netology.ru/microsoft

Курс "Управление безопасностью в малом и среднем бизнесе". Он содержит следующие темы:

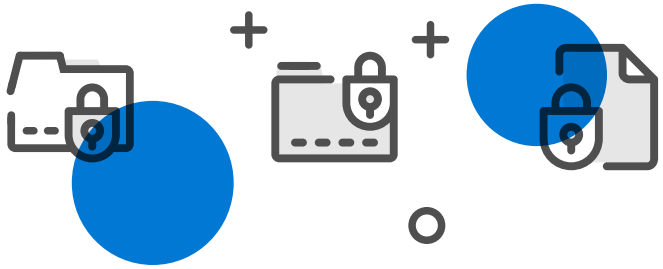
— Настройка и управление возможностями безопасности в Windows 10

— Конфигурации Advanced Threat Protection для малой и средней компании

— Защита информации с помощью Azure Information Protection, Data Leak Protection

— Управление устройствами с помощью Microsoft Intune

— Защита от шифровальщиков и миграция файлового хранилища в OneDrive для Бизнеса




Microsoft