Главная тема

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Сергей ХАЛЯПИН,
руководитель отдела системных инженеров Citrix в России и странах СНГ

ПРИНЦИПЫ БЕЗОПАСНОСТИ И ТРЕБОВАНИЯ БУДУЩЕГО

Сегодня задача защиты данных требует от специалистов по информационной безопасности владения принципиально новым набором профессиональных навыков. Речь идет о согласованном управлении сетевыми технологиями, чтобы предоставить сотрудникам как гибкость для работы в любом месте, так и обеспечение надежной защиты персональных и служебных данных.

Новая модель обеспечения безопасности выглядит следующим образом: вместо сохранения и управления всеми элементами инфраструктуры, включая приложения, данные, сеть, систему хранения данных и серверы, сотрудникам предоставляется возможность применять собственные устройства для доступа к данным и приложениям, даже с использованием публичных сетей. Будут задействованы облачные сервисы и SaaS-решения, управляемые сторонними компаниями и размещенные у них, поэтому собственный центр обработки данных компании станет всего лишь одним из узлов постоянно расширяющейся гибридной среды. И это будет происходить даже с учетом усиления угроз.

Неудивительно, что специалисты по информационной безопасности в финансовой сфере, в сфере здравоохранения и других отраслях проявляют всё большую озабоченность. Подобная ситуация наблюдается

во всех компаниях, которые хотят защитить свои данные. Но суровая правда заключается в том, что нельзя вернуться во времена, когда использовались единые информационные технологии, закрытые сети, а сотрудники были привязаны к своим рабочим местам. И нет никакого смысла держаться за модели обеспечения безопасности того времени — они просто не работают сейчас. В условиях, когда мобильность является ключевым требованием бизнеса, а ориентирование информационных технологий на потребителя изменяет представление людей об используемых ими решениях, необходимо пересмотреть вопросы безопасности в соответствии с новыми требованиями.

Информационные технологии столкнулись с двумя взаимосвязанными задачами:

- **Удовлетворение потребностей сотрудников** — на основании потребностей бизнеса — для обеспечения гибкости и мобильности с возможностью работать на любом устройстве, в любом месте, по любой сети и при наличии локальных, облачных и мобильных приложений и сервисов.
- **Решение вопросов, связанных с уязвимостью** частной информации, коммерческой тайны, интеллектуальной собственности и других важных данных по основным направлениям: контроль доступа, уязвимости приложений, а также физической и социальной инженерии. Кроме того, необходимо обеспечить защиту при хранении, передаче и использовании как на серверах, так и на устройствах.

Важность обеих задач трудно переоценить. Активное развитие цифровых технологий приводит к быстрому увеличению объемов данных компаний. Этот процесс также сопровождается ростом количества утечек данных, потерь и краж важной информации. Кроме того, стоит отметить, что даже самый надежный периметр защиты не может уберечь от ошибок, вызванных человеческим фактором, а также от желания сотрудников компании навредить работодателю.

Одним из преимуществ старой модели обеспечения защиты являлась ее простота: после входа в систему с помощью корпоративной учетной записи можно было использовать всю имеющуюся информацию. Конечно, обратной стороной этой простоты становились утечки данных и резонансные атаки.

Новая модель должна быть такой же простой, но защищать данные в соответствии с современными принципами работы. Важно применять контекстный подход к проблеме доступа к информации. Для решения этой проблемы необходимо задать себе пять вопросов:

1. **Кто** пытается получить доступ к данным?
2. **К каким** данным он пытается получить доступ?
3. **Что** происходит при доступе к данным?
4. **Где** находится пользователь?
5. **Зачем** ему нужен доступ?

Ответив на эти вопросы, ИТ-специалисты смогут принять правильное решение о предоставлении доступа к данным. Более того, ИТ-департамент сможет даже автоматизировать этот процесс, исходя из профиля сотрудника и опыта

> Нельзя вернуться во времена, когда использовались единые информационные технологии и закрытые сети — и нет смысла держаться за модели обеспечения безопасности того времени

ДОСЬЕ

Сергей ХАЛЯПИН

В компании Citrix начал работать в 2007 году на позиции системного инженера. В настоящее время является официальным техническим представителем компании. Отвечает за обучение и повышение квалификации инженерного состава партнеров и дистрибьюторов, тестирование решений и работу с технологическими партнерами. Имеет сертификаты компаний Citrix Systems, Cisco, COMPTIA, Microsoft и Symantec.

прошлых запросов доступа. Новые модели безопасности, которые учитывают эти пять вопросов, имеют высокий уровень адаптивности и могут подать сигнал тревоги, если кто-то пытается подключиться, используя неизвестное устройство или из неизвестного места. Проверка не ограничивается определением вашей подлинности с помощью пароля и идентификационных данных. В доступе к данным может быть отказано, если цель или условия доступа не соответствуют установленным. При принятии решения учитываются все пять факторов.

Так, например, вопрос «кто» должен рассматриваться, исходя из ответа на вопрос «что». Доступ к более важным данным подразумевает более серьезную систему авторизации, более частые проверки и более строгие политики. Система многофакторной аутентификации не будет применяться в отношении сотрудников, занимающих должности начального уровня, но при предоставлении доступа к наиболее важной информации будут использованы системы распознавания черт лица пользователя и проверка биометрических данных. Определенные транзакции могут быть ограничены только определенными системами и сетями.

Вопрос «кто» также должен быть проверен на соответствие ответам на вопросы «когда» и «где». Сотрудник впервые входит в учетную запись в 3:30 утра? Пытается получить доступ к важным данным из другой страны? Запрашиваемые данные относятся к другому подразделению компании или проекту? Отличие от обычных характеристик не обязательно приведет к запрету доступа, но вызовет дальнейшую проверку.

Система также должна иметь ответ на вопрос «почему» и предикативную способность понимать на основании расписаний и маршрутов передвижения, в каком месте сотрудникам потребуется доступ в будущем, или как изменятся требования при изменении должностной роли сотрудника в компании. Это поможет уменьшить потребность в привлечении технических специалистов и избежать неудобств в работе персонала.

Данные и люди становятся всё более мобильными, поэтому финальные элементы новой модели обеспечения безопасности — шифрование и контролируемость — помогают защитить организации от любых рисков в любой ситуации. Данные должны быть зашифрованы как при хранении, так и при передаче, для того чтобы даже нарушение политик или процессов не привело к их раскрытию. Для внутреннего анализа и обеспечения соответствия нормативным требованиям необходимо проверять и вести журнал для каждой транзакции, чтобы полностью контролировать доступ к данным.

Простая, но при этом комплексная модель контекстного доступа к информации имеет дополнительное преимущество в виде использования релевантных и независимых факторов. Объединение мобильности и гибкости с детальным управлением и контекстным доступом позволяет более эффективно использовать данные для повышения продуктивности.

ГЛОССАРИЙ

SaaS

(англ. software as a service — программное обеспечение как услуга; также англ. software on demand — программное обеспечение по требованию)

Бизнес-модель продажи и использования программного обеспечения, при которой поставщик разрабатывает веб-приложение и самостоятельно управляет им, предоставляя заказчику доступ к программному обеспечению через интернет. Основное преимущество модели SaaS для потребителя услуги состоит в отсутствии затрат, связанных с установкой, обновлением и поддержкой работоспособности оборудования и работающего на нем программного обеспечения.

> Данные и люди становятся всё более мобильными, поэтому новая модель обеспечения безопасности помогает защитить организации от любых рисков и в любой ситуации