Жан-Ноэль де Гальзан, CEO WALLIX: «Комплексная политика безопасности должна включать эффективное управление привилегированными пользователями»

В последние годы организации, равно как и индивидуальные пользователи, вынуждены много времени посвящать обеспечению кибербезопасности. Однако, несмотря на все усилия, прикладываемые в этом направлении, количество угроз не только не уменьшается, но продолжает расти! Атаки становятся более целенаправленными, разнообразными и сложными. Киберпреступность сегодня является частью нашей повседневной жизни.

Традиционно на рынке средств киберзащиты доминировали поставщики антивирусов и межсетевых экранов. Однако подобные решения позволяют устранить лишь часть проблем: дело все в том, что поставщики таких продуктов упускают из виду важный аспект ИТ-безопасности — управление «внутренними» угрозами.

Компания WALLIX, европейский лидер в сфере технологий отслеживания и управления привилегированными пользователями, считает, что комплексная стратегия обеспечения безопасности должна учитывать не только внешние угрозы, но также риски, связанные с действиями привилегированных пользователей.

Кто такой привилегированный пользователь?

Привилегированный пользователь имеет расширенные права в отношении доступа, управления авторизацией, администрирования устройств и приложений, изменения, удаления или передачи файлов. Привилегированными пользователями могут быть сотрудники компании или ее внешнего подрядчика. Их права определяются руководителями, которые зачастую не осведомлены о рисках, связанных с таким уровнем

полномочий. Привилегированные пользователи зачастую имеют доступ к важным, имеющим стратегическое значение, данным, а также к конфиденциальной информации о компании или ее сотрудниках. Иными словами, в их руках — жизнь и смерть бизнеса.

Всегда ли привилегированный пользователь является сотрудником компании?
Если компания передает управление всей ИТ-инфраструктурой или ее частью сторонним поставщикам, которые удаленно контролируют или работают во внутренней сети, такие поставщики становятся привилегированными пользователями, хотя они не являются сотрудниками компании. Знаете ли вы, например, какими правами доступа обладает технический специалист, который занимается ремонтом копировальных устройств или решает проблемы с подключением к сети?
Иными словами, аутсорсинг зачастую можно сравнить с передачей ключей от офиса незнакомцу, который может войти в любую комнату и открыть любой шкаф, обыскать вещи и забрать все, что найдет. Если что-то было повреждено, пропало или украдено, какие меры следует предпринять? Как узнать, что случилось? В чем причина происшедшего? Когда это произошло? И каким образом? Кто заплатит за нанесенный ущерб? Какие материалы я могу предоставить страховой компании, чтобы доказать факт кражи или инцидента?

Какие риски связаны с деятельностью привилегированных пользователей?
Именно вследствие своего высокого статуса привилегированные пользователи могут своей деятельностью создавать огромные риски для организации. Эти риски можно разделить на следующие категории:

- Банальные ошибки: как и любой другой человек, привилегированный пользователь не застрахован от ошибок, которые могут иметь серьезные последствия для производительности, репутации и финансовой состоятельности компании.

- Представьте себе такую ситуацию: внешний поставщик услуг совершает ошибку в процессе удаленного технического обслуживания веб-сервера, в результате чего сервер выходит из строя. Компания, занимающаяся электронной торговлей, будет нести финансовые потери, пока не будет выявлена причина и неисправность не будет устранена. Это может занять немало времени и нанести ущерб репутации компании. Не говоря уже о том, что к тому времени, как проблема будет решена, многие клиенты уже обратятся к другому трейдеру.

- В соответствии с современными нормативами организации должны отчитываться о любых инцидентах и рисках, связанных с потерей информации о клиентах (персональные данные, номера дебетовых и кредитных карт или сведения о состоянии здоровья). Не так давно был случай, когда сотни медицинских карт были опубликованы в Интернете. Это выяснилось, только когда человек ввел свое имя в поисковой системе и обнаружил, что его медицинская карта доступна для любого пользователя. Подобного рода утечки информации могут быть следствием как человеческой ошибки (несоблюдения внешним

поставщиком услуг процессов управления информацией), так и целенаправленных действий злоумышленников.

- Недовольные сотрудники: привилегированным пользователям, как всем людям, свойственны различные эмоции. Привилегированный пользователь, которого несправедливо, как он считает, увольняют, может попытаться в отместку воспользовать своими расширенными правами, чтобы навредить компании или похитить важную информацию (сведения о клиентах, номера дебетовых и кредитных карт, секретные материалы и т. д.).
  Например, в 2012 году субподрядчик компании Toyota, договор с которым был расторгнут, похитил информацию о патентах японского производителя автомобилей. Руководителям Toyota пришлось спешно искать ответы на малоприятные вопросы: Сколько записей баз данных было украдено и сколько материалов было раскрыто? Какой объем информации был извлечен из незаконно скачанных файлов? Кто сделал это? Когда и как? Почему этот человек имел доступ к этим данным? Можно ли предотвратить такие инциденты или регистрировать все подобные действия? Как можно контролировать действия сотрудников и внешних поставщиков услуг?
  Согласно результатам опроса Forrester, 50 процентов привилегированных пользователей уходят из компаний с конфиденциальными данными на руках. Как же можно достичь высокой эффективности управления рисками, не имея возможности контролировать действия привилегированных пользователей?
  К счастью, все больше ИТ-отделов и директоров по ИТ-безопасности используют решения, которые позволяют управлять как внутренними угрозами, так и угрозами, исходящими от внешних поставщиков услуг. Они интегрируют решения по управлению привилегированными пользователями в свои политики обеспечения безопасности.
  Однако, несмотря на злободневность проблемы, рынок решений для управления привилегированными пользователями еще сравнительно молод.
  Компания WALLIX, пионер в сфере технологий управления привилегированными пользователями и разработчик решения Wallix AdminBastion, безусловно, рекомендует компаниям защищаться от угроз, возникающих за пределами сети. Эти угрозы хорошо известны, и с ними успешно справляются такие средства, как антивирусы, межсетевые экраны, системы обнаружения и предотвращения вторжений. Поэтому компания WALLIX акцентирует внимание на необходимости использовать дополнительно решения для контроля действий внутренних привилегированных пользователей.
  Вместе с тем, многие относятся к подобным решениям скептически: часто они воспринимаются как продукты, созданные просто-напросто для мониторинга работы привилегированных пользователей. Вопреки ожиданиям, они зачастую освобождают от ответственности этих пользователей, предоставляя конкретные доказательства настоящих причин инцидента.
  Жан-Ноэль де Гальзан (Jean-Noël de Galzain), основатель и CEO компании WALLIX, говорит: «Комплексная и эффективная стратегия обеспечения безопасности не может обойтись без решений для управления привилегированными пользователями. Каждый день привилегированные пользователи получают доступ к данным, от которых в

значительной степени зависит судьба компании. Злонамеренные действия пользователей, конечно, не единственная причина утечки данных. Существует также вероятность человеческой ошибки, которая в некоторых случаях может приводить к катастрофическим последствиям. Руководители ИТ-отделов и директора по ИТ-безопасности должны осознавать, какой ущерб могут нанести привилегированные пользователи в плане производительности, репутации и соответствия нормативным требованиям. Именно поэтому я уверен: управлению внутренними рисками надо уделять не меньшее внимание, чем внешним угрозам».
Компания WALLIX предлагает инновационные решения для отслеживания и контроля доступа к ИТ-инфраструктуре. Одним из таких решений является платформа Wallix AdminBastion, которая позволяет управлять доступом привилегированных пользователей. Wallix AdminBastion служит в качестве защитного барьера для привилегированных пользователей и позволяет записывать все их действия для последующего просмотра с целью определения причины инцидента. Кроме того, данное решение помогает соблюдать требования стандартов в сфере ИТ-безопасности, таких как PCI DSS, SOX, Basel II и т. п. Развертывание Wallix AdminBastion не представляет никаких трудностей, а для его использования не требуется устанавливать агент. Вы сможете начать работу уже через несколько часов.

Жан-Ноэль де Гальзан, CEO WALLIX

О компании Wallix

Компания WALLIX — это европейский лидер в сфере технологий информационной безопасности. Мы объединили три основных области управления привилегированными пользователями (управление паролями, контроль доступа и функции отслеживания) в единое, удобное в развертывании решение — Wallix AdminBastion (WAB).

Дистрибьюторская сеть WALLIX охватывает страны Европы, Ближнего Востока, Африки и Северной Америки. Продукты WALLIX призваны помочь современным организациям из разных отраслей обеспечить выполнение самых разных нормативных требований. Представительства WALLIX открыты во Франции, Великобритании и США, а клиентская аудитория компании охватывает весь земной шар.

WALLIX является признанным инноватором в своей области. За годы работы компания удостоилась множества сертификатов и наград, в том числе Oseo Excellence, Systematic Paris-Region Systems и ICT Cluster Champion, а также стала победителем программы PM'UP региона Иль-де-Франс (программа поддержки 200 SME-компаний с наиболее высоким технологическим потенциалом). Поддержку компании осуществляют инвестиционные фонды Access2Net, Sopromec, Auriga Partners, TDH, а также французский государственный фонд FSN (Fond national pour la Societe Numerique).