# «РАМ КАК КОНТРОЛИРУЕМЫЕ ВОРОТА В ИНФРАСТРУКТУРУ»

***Только за первый квартал 2024 года в РФ объем утекших данных среди организаций в сегменте малого и среднего бизнеса вырос почти в четыре раза по сравнению с аналогичным периодом прошлого года, подсчитали в «Лаборатории Касперского». При этом бизнес стал более внимателен к защите критически важных данных. О том, как системы класса PAM (Privileged Access Management) помогают решать вопросы кибербезопасности, о ситуации на российском IT-рынке после ухода зарубежных вендоров и дефиците кадров в отрасли рассказал генеральный директор компании «АйТи Бастион» Сергей Бочкарев.***

**— Общая тенденция 2023–2024 годов — все более упорядоченные атаки хакеров на критическую инфраструктуру. Как системы контроля привилегированных пользователей (PAM) помогают госкомпаниям и частному бизнесу решать вопросы безопасности?**

— Театр начинается с вешалки, а контроль удаленного доступа к критически важным инфраструктурам начинается с PAM. Потому что PAM-система является той самой отправной точкой по контролю конкретного человека.

Зачастую в организациях не ставят защиту на целевую систему, потому что какие-либо дополнительные программы расходуют слишком много ресурсов и влияют на производительность той самой критической системы. Не в 100% случаях, но часто такие системы оставляют без полезных агентов безопасности, к которым необходимо подключение. Система работает — и ладно... Что же в ней происходит после подключения тех или иных администраторов, остается неизвестным.

Когда же в компании есть платформа по контролю привилегированных пользователей (PAM), каждое соединение валидируется, собираются данные о событиях информационной безопасности, фиксируются отклонения от привычной деятельности администратора внутри критической системы. Фактически PAM — это контролируемые ворота в инфраструктуру.

В условиях повсеместной удаленной работы такие средства информационной безопасности стали основой защиты от цифровых неприятностей «внутри контура» как для больших организаций, так и для развивающегося бизнеса.

Технологии платформы СКДПУ НТ (https://it-bastion.com/produkt/skdpu-nt), над которыми работает наша компания, не только безопасно приводят нужного пользователя в значимую инфраструктуру, но и ограничивают его деятельность уже внутри системы. Пользователь с минимальными полномочиями несет меньший риск, а если для решения конкретного задания ему понадобились повышенные права, то PAM позволяет их оперативно предоставить без привлечения дополнительных ресурсов IT-служб по написанию служебных записок.

**— Одна из проблем, с которой сталкивается бизнес сегодня,— это утечки данных от пользователей внутренних систем (сотрудников или контрагентов). Как технология решает эту задачу? Какие инструменты наиболее эффективны?**

— В ситуации «тотального гибрида» решение PAM позволяет контролировать все соединения и четко понимать, что происходит во время этих соединений. Понятно, что PAM-система не рассматривается как панацея, современной инфраструктуре нужны средства защиты от утечек данных, системы контроля баз данных, конфигураций. Ведь смысл разумной и правильной безопасности состоит в том, чтобы обеспечить работоспособность комплекса IT- и ИБ-систем.

Безусловно, PAM входит в ядро стека кибербезопасности. И мы как разработчик стараемся предоставить заказчикам не только продукт класса PAM, но и возможности быстро интегрировать его с соседними системами — для обогащения данными, упрощения



взаимодействия пользователя с информацией по безопасности, повышения скорости и качества анализа.

**— Сложнее ли выявить утечку данных, если сотрудник работает вне офиса, на удаленке?**

— Все зависит от самого пользователя, точнее, от того, как организовано его удаленное подключение. Очень сложно уследить за администратором, когда ему выдали ключ от VPN, а он установил его на личный ноутбук, на котором нет достаточного количества средств информационной защиты. В идеальной картине мира сотрудник даже вне офиса работает в корпоративной среде через зашифрованные соединения и многоуровневую проверку конкретного рабочего места.

Рабочие места в офисе не требуют такого пристального внимания, с ними все проще и понятнее. Поэтому одно из распространенных решений — подключение георазпределенных специалистов к некоей рабочей станции внутри компании, которая выполняет функцию джамп-сервера. И только через этот хост можно взаимодействовать с внутренней инфраструктурой.

Одним из вариантов реализации сценария как раз являются PAM-системы. В общей архитектуре они выступают промежуточным звеном, позволяющим не только записывать события, но и изолировать потенциально небезопасную рабочую станцию пользователя от корпоративной инфраструктуры.

**— Какой объем занимает сегмент PAM на российском IT-рынке сегодня?**

— Еще четыре года назад сегменту PAM прогнозировали бурный рост с перспективой покинуть список нишевых продуктов информационной безопасности — пандемия значительно раздвинула границы рынка. Но произошли геополитические изменения, повлекшие за собой перераспределение ресурсов заказчиков в сторону базовых систем кибербезопасности. Всем необходимо импортозаместить решения класса SIEM, Endpoint, XDR, NGFW.

Мы можем смело говорить о нескольких миллиардах рублей в рынке, но считать будем по осени. Уверен, что в 2025 году появятся наглядные срезы рынка PAM по итогам текущего и прошлых годов.

**— Как изменился рынок решений для управления доступом за последние несколько лет, в том числе после ухода из РФ иностранных вендоров?**

— Большинство крупных компаний уже перешли или находятся в процессе перехода на российские решения. Заказчики поняли, что обратного пути нет. Доверие к иностранным вендорам минимальное, и нет никакого смысла ждать их возвращения обратно. Нам нужно работать здесь и сейчас.

В сегменте управления доступами появились нишевые разработчики, что раньше было редкостью. Большинство из них предлагают продукт исключительно под отечественные операционные системы, понимая, что со временем заказчики просто не смогут работать на Windows, потому что это небезопасно. Очень надеюсь, что новые игроки сделают все честно, а не для галочки, когда сертифицируют систему управления на Astra, а «под капотом» остается Windows.

**— В каких отраслях экономики системы PAM наиболее востребованы? Чем это обусловлено?**

— Спрос на СКДПУ НТ стабильно увеличивается во всех отраслях, растет число «пилотов» и проектов. К крупным организациям госсектора, промышленности и нефтегазового блока, а также финансов присоединились такие заказчики, как аэропорты, спортивные организации, многопрофильные холдинги — все они обратили внимание на выгоду и необходимость приобретения PAM-системы.

В целом многие компании начали уделять внимание внутренней безопасности — для подключения внешних подрядчиков, удаленной работы, обеспечения защищенной разработки.

Если говорить о малом и среднем бизнесе, то уровень ответственности за информационную безопасность у них сравнялся с крупными игроками. СМБ часто находятся на подряде у больших компаний, являясь поставщиками услуг, поэтому, взломав их, легче войти в инфраструктуру энтерпрайза. Сами посудите, зачем пытаться взломать дверь, если проще проникнуть внутрь через открытое окно. Вот такими «открытыми окнами» сейчас и являются СМБ-компании, которые в большинстве своем отстают в вопросах обеспечения внутренней кибербезопасности.

**— Ответственность за утечки персональных данных в следующем году может значительно ужесточиться. Сейчас в Госдуме рассматривают законопроект, который предполагает увеличение штрафов за нарушения при работе с персональными данными. Как нововведение повлияет на рынок?**

— Если правовое поле будет достаточно урегулировано и не останется возможностей для ухода из-под штрафов, то, конечно, разработчикам PAM это на руку. Весь рынок ждет, как новое законодательство будет реализовано на практике. Пока что проблема утечки персональной информации остается личным горем граждан, а не ответственностью государства или организации, допустившей кражу данных.

**— В IT, как и в других сферах, уже не первый год наблюдается дефицит кадров. Ощутима ли проблема в сегменте PAM? Как ее решаете?**

— Привлечь хорошего специалиста всегда сложно, но мы справляемся и находим только настоящие таланты. Как показала практика, лучше это делать самостоятельно под нашу задачу. Например, мы заключили соглашение о сотрудничестве с московским Политехом, и это сразу дало результаты. Сначала в отделах появилось несколько перспективных студентов-практикантов, а сейчас они уже молодые специалисты в штате — показатель перехода со стажировки на постоянную роль в команде составил 100%!

В целом же отрасль информационной безопасности во всем мире испытывает дефицит кадров, и счет здесь идет на миллионы специалистов. Чтобы дефицит не превратился в голод, работать над результатом необходимо всем вместе: государству, системе образования, компаниям-разработчикам и корпоративному бизнесу.

РЕКЛАМА, 12+