КОГДА МАЛЫЙ БИЗНЕС СТАНОВИТСЯ БОЛЬШОЙ МИШЕНЬЮ

Киберпреступность давно вышла за рамки «большой игры». Сегодня в фокусе злоумышленников — малый и средний бизнес. Ресурсов там меньше, а вот данные не менее ценные: от клиентских баз до доступа к сервисам. Одна атака способна надолго выбить компанию из колеи, повлечь убытки, проверки и репутационные потери. В таких условиях информационная безопасность — уже не роскошь, а реальная необходимость. Но как защититься, если нет своей ИБ-службы, многомиллионного бюджета и времени на сложные внедрения? Об этом рассказал Константин Родин, заместитель директора по развитию бизнеса компании «АйТи Бастион».

— Насколько актуальна сегодня тема информационной безопасности для малого и среднего бизнеса?

— Актуальность этой проблемы сложно переоценить. Так было всегда, но если раньше основными мишенями киберпреступников были крупные корпорации, то сегодня малый и средний бизнес как никогда «под прицелом». Причина — в ограниченных ресурсах и отсутствии выстроенной ИБ-инфраструктуры. Компании часто вынуждены выбирать между затратами на развитие бизнеса и инвестициями в безопасность. В результате растет риск инцидентов: от утечек персональных данных до компрометации корпоративных систем. При этом последствия именно для небольших компаний могут быть критичными: от штрафов до потери клиентов и репутации.

— Почему МСБ нередко не уделяет достаточного внимания информационной безопасности?

— Причин несколько. Во-первых, ограниченные бюджеты. Во-вторых, нехватка ИТ-экспертизы внутри команды. Нередко ИБ-вопросами занимаются один-два специалиста, а иногда вообще никто — это делегируется на внешний аутсорс. А злоумышленники очень хорошо натренировались на крупных корпорациях, да и технологии на месте не стоят. Стоимость атаки неуклонно снижается. В-третьих, отсутствует понимание, что угрозы реальны. Пока не произойдет инцидент, вопрос безопасности, увы, воспринимается как «второстепенный». Мы стремимся изменить этот подход, предлагая решения, которые учитывают возможности и специфику малого бизнеса.

— Что вы имеете в виду под «спецификой»? В чем отличия защиты ИТ-инфраструктуры малого бизнеса от крупного?

— Очевидно, что основное отличие — в масштабе и гибкости. У МСБ нет собственных ЦОД и распределенных команд ИБ, как у корпораций. Инфраструктура, как правило, размещается на аутсорсинге или в облаке, доступ к системам получают подрядчики, а администрирование нередко совмещается с другими функциями. Поэтому ключевыми становятся простота внедрения, низкий порог входа и высокая эффективность даже при минимальных ресурсах. Именно под такие запросы и был разработан наш новый продукт — СКДПУ НТ Старт, выход которого мы на днях анонсировали.

— Расскажите, что представляет собой это решение и чем оно отличается от флагманского?

— СКДПУ НТ Старт — это легкий вариант нашей основной PAM-платформы СКДПУ НТ, адаптированный под возможности и потребности малого и среднего бизнеса. Он предоставляет базовый, но достаточный набор функций: контроль привилегированного доступа, запись сессий, гибкое разграничение прав через ролевую модель, автоматический анализ активности пользователей, автоматические блокировки нежелательных действий. В отличие от «большого» СКДПУ НТ, который рассчитан на крупные компании с комплексной инфраструктурой (в том числе и на объекты КИИ), Старт не требует длительного внедрения и может быть полностью развернут в срок до четырех часов. Образно говоря, это своего рода «входной билет» в мир PAM-решений — зрелый, но доступный и практичный.



— Каковы основные риски, с которыми сталкивается МСБ при работе с подрядчиками и удаленными администраторами?

— Не секрет, что один из главных рисков — отсутствие контроля. Подрядчику или временно привлеченному специалисту часто выдаются максимальные привилегии, и даже после завершения проекта этот доступ остается (удивительно, но факт!). Нет логирования действий, не видно, кто, когда и зачем подключался. В результате этот специалист (не обязательно, конечно, злоумышленник) может вернуться спустя какое-то время и использовать «открытые двери» для каких-то своих целей. СКДПУ НТ Старт устраняет эту проблему: все действия фиксируются, доступ управляется централизованно, можно ограничить время, IP, команды — все прозрачно и управляемо. И даже если спустя месяц вы решили проверить, не оставил ли он вам «подарок», это легко можно сделать, просмотрев журналы событий и видео его работы на компьютере.

— Система фиксирует действия пользователей. Насколько глубоко это реализовано?

— В СКДПУ НТ Старт реализована полноценная система записи сессий: видеопоток и текстовая команда. Это значит, что можно не только просматривать действия в интерфейсе, но и проанализировать, какие именно команды были выполнены. Дополнительно встроены механизмы анализа сетевых команд: если пользователь вводит потенциально опасную команду или запускает несанкционированное приложение — система может немедленно заблокировать его действия или оповестить администратора. Мы реализовали механизмы, которые позволяют видеть даже запущенные или остановленные процессы на целевой системе. Какие будут ваши действия, если бы вы увидели, что процесс вашего антивируса был завершен пользователем? Я бы немедленно отреагировал.

— Как происходит внедрение системы и сколько времени оно занимает?

— Ключевая идея — это простота. Интеграция, как я уже сказал, занимает от одного до четырех часов. Не требуется глубоких технических знаний или вмешательства в ИТ-инфраструктуру. Мы предусмотрели типовые сценарии, которые позволяют быстро развернуть систему даже без штатного ИБ-специалиста. Это особенно важно для компаний, у которых нет возможности выделить команду на длительный проект.

— Какие задачи автоматизирует СКДПУ НТ Старт?

— Они разные. Во-первых, это автоматическое предоставление и отзыв доступа — из работы исключается «человеческий фактор». Во-вторых, система сама выявляет нежелательную активность и может инициировать блокировку или уведомление. Это особенно полезно в условиях высокой текучести кадров — новички или уволенные сотрудники не смогут использовать старые учетные данные. Кроме того, ведется непрерывный аудит действий, который упрощает внутренние проверки и подготовку отчетности в дальнейшем.

— Есть ли у СКДПУ НТ Старт сертификат ФСТЭК, чтобы его можно было использовать в компаниях?

— Сертификат ФСТЭК на СКДПУ НТ Старт мы не предоставляем. У него другое назначение — обеспечить защиту «здесь и сейчас». Считаю это важным преимуществом именно для малого и среднего бизнеса. Благодаря этому Старт можно быстро внедрять без лишней бюрократии, согласований и затрат. Сертифицированные решения — это, безусловно, важно для госсектора и объектов КИИ, но для МСБ зачастую именно это становится барьером: долго, сложно, дорого. Наш продукт создан именно как легкое, практичное решение. Но при этом оно полностью отвечает требованиям здравого смысла и базовым мерам по ИБ. А если бизнес вырастет и появится необходимость в сертифицированной версии, то у нас есть основное решение СКДПУ НТ, на которое можно потом перейти на максимально выгодных условиях.

— А насколько Старт устойчив к внутренним угрозам?

— Действительно, очень часто киберугрозы исходят не извне, а изнутри: недобросовестный сотрудник, случайная ошибка, незакрытый доступ. СКДПУ НТ Старт позволяет свести такие риски к минимуму. Благодаря блокировке опасных команд и приложений, контролю действий в реальном времени и записи всех сессий поведение каждого пользователя можно отследить и проанализировать. Это не только превентивная защита, но и мощный инструмент реагирования.

— С какими типичными ошибками в безопасности чаще всего сталкиваются компании из сегмента МСБ?

— Прежде всего — это отсутствие учета и контроля доступа. Люди работают под одним логином, доступы не пересматриваются годами, логов нет. Также часто используются устаревшие средства: пароли в Excel единым списком, удаленный доступ через неконтролируемые ПО. Все это создает иллюзию безопасности и эффективности. Наша задача — дать бизнесу простой инструмент, который поможет закрыть эти уязвимости без излишней сложности.

— Планируется ли расширение функциональности СКДПУ НТ Старт в будущем?

— Конечно. Мы активно собираем обратную связь от наших партнеров и заказчиков. Уже сейчас в планах — интеграция с другими решениями по ИБ, расширение взаимодействия по API с корпоративными системами и расширенные отчеты. Но важный принцип остается: система должна оставаться простой и доступной для небольших команд. И иметь, разумеется, потенциал роста.

— Что бы вы посоветовали компаниям, которые только задумываются о защите IT-инфраструктуры?

— Мой совет прост: не надо откладывать. Информационная безопасность — это не роскошь, а базовая необходимость. Даже один инцидент может обернуться катастрофой для бизнеса. Лучше сделать первый шаг, чем бесконечно откладывать путь из-за его кажущейся сложности. Мы предлагаем начать с самого важного — с контроля критически важных для бизнеса систем. А именно — с управления привилегированным доступом, ведь именно здесь сосредоточены наибольшие риски. Дальше — постепенно выстраивать систему безопасности по мере роста бизнеса и требований. Со своей стороны, мы готовы предложить решения, которые соответствуют реальным возможностям компаний и при этом надежно защищают их данные.

РЕКЛАМА, 12+