УГРОЗЫ КИБЕРБЕЗОПАСНОСТИ ДЛЯ МАЛОГО И СРЕДНЕГО БИЗНЕСА

МИШЕНЬЮ ХАКЕРСКИХ И ВИРУСНЫХ АТАК, КАК ПРАВИЛО, СТАНОВЯТСЯ КРУПНЫЕ КОРПОРАЦИИ И ПРАВИТЕЛЬСТВЕННЫЕ ОРГАНИЗАЦИИ. НО СЕЙЧАС СИТУАЦИЯ МЕНЯЕТСЯ: 20% АТАК СОВЕРШАЕТСЯ НА КОМПАНИИ МАЛОГО И СРЕДНЕГО БИЗНЕСА (МСБ). ЕСЛИ КРУПНЫЙ БИЗНЕС И ГОСУДАРСТВО УЖЕ ДОСТАТОЧНО ЗАЩИТИЛИ СВОЙ IT-ПЕРИМЕТР, ТО КОМПАНИИ МСБ ЗАЩИЩЕНЫ ХУЖЕ. АЛЛА МИХЕЕНКО

Между тем одной из тенденций прошлого года было не просто увеличение кибератак, а бесцельное поражение хакерами любых систем с желанием подорвать работу в бизнес-секторе вне зависимости от его масштаба деятельности. Как обезопасить себя и с какими еще рисками могут столкнуться представители МСБ, рассказали специалисты компании «АйТи Бастион».

«АЙТИ БАСТИОН»

ПЕРВЫЙ ШАГ К ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ — ПОНИМАТЬ, ЧТО ДЕЛАЮТ АДМИНИСТРАТОРЫ И ПОДРЯДЧИКИ КОМПАНИИ, КОТОРЫЕ ИМЕЮТ ДОСТУП К КРИТИЧЕСКИ ВАЖНЫМ РЕСУРСАМ

РОСТ УГРОЗ В январе 2022 года вице-премьер Дмитрий Чернышенко заявлял, что за 2022 год было отражено около 50 тыс. хакерских атак на отечественные интернет-ресурсы, число атак на автоматизированные системы управления увеличилось почти в два раза по сравнению с 2021 годом. В основном удар пришелся на госсектор, однако каждая пятая атака пришлась на предприятия малого и среднего бизнеса. В первом квартале 2023 года эксперты также отмечали рост кибератак на 60% по сравнению с аналогичным периодом прошлого года. Так, в январе — марте 2023 года было зафиксировано около 290 тыс. кибератак, приводит данные ТАСС со ссылкой на отчет «РТК-Солар». Специалисты отмечают, что хакеры чаще стали прибегать к киберразведке, а атаки становятся все более сложными.

Эксперты сходятся во мнении, что информационная безопасность остается одним из важнейших векторов цифрового развития. А позаботиться о ней нужно не только крупным игрокам, но и предприятиям малого и среднего бизнеса.

«С одной стороны, в России не принято рассказывать о взломах и утечках, хвастаться нечем, и бизнес такие инциденты скрывает. С другой стороны, часто компании узнают о том, что данные их сотрудников или клиентов утекли, только из публикаций в СМИ. Базы данных размещают в даркнете, специалисты анализируют их и определяют, чье это. Так, все чаще появляется информация о том, что злоумышленники украли и продают базу пациентов медицинских центров, служб доставки, даже агентств недвижимости. При этом 50% информации, продаваемой в даркнете,— это доступы к инфраструктуре той или иной компании. То есть даже хакером не надо быть, просто покупаешь логин-пароль, заходишь хотя бы на сайт компании и делаешь там что хочешь. Собственно, все эти ситуации возможны из-за того, что небольшой бизнес не контролирует доступ к своим информационным ресурсам, не знает, что делают их собственные и привлеченные IT-администраторы. И вообще не думает об информационной безопасности»,— комментирует генеральный директор компании «АйТи Бастион» Сергей Бочкарев.

ПОСЛЕДСТВИЯ КИБЕРАТАК Зачастую руководитель компании малого или среднего бизнеса ставит задачу обеспечения информационной безопасности на второй план, так как не имеет глубокого представления о современных киберугрозах и их последствиях. Мишенью хакерских атак могут быть базы данных с контактами клиентов, бизнес-идеи и стратегии, банковские операции, производственные процессы и ценовая политика, личные данные сотрудников. Кража информации чревата финансовыми потерями и репутационным ущербом. В результате кибератака может обернуться закрытием бизнеса, так как восстановление слишком затратное. Есть случаи, когда малые предприятия, ставшие жертвами атаки, закрываются в течение полугода после инцидента.

Одна из самых серьезных угроз — это попытки взлома через скомпрометированный сервер компании ресурсов государственных органов. Фирмы обнаруживали, что их взломали тогда, когда к ним приезжали спецслужбы для бесед и изъятия оборудования.

КАК СЕБЯ ОБЕЗОПАСИТЬ? Бизнес может стать целью для киберпреступников — это лишь вопрос времени. Важно задуматься о надежной защите, и одной антивирусной программой здесь не обойтись. Первый шаг к информационной безопасности — понимать, что делают администраторы и подрядчики компании, которые имеют доступ к критически важным ресурсам.

Для организаций с небольшой IT-структурой и ограниченным бюджетом на информационную безопасность «АйТи Бастион» разработал продукт — «СКДПУ НТ Компакт», который обеспечивает полный функционал контроля внутренних и внешних администраторов. Программа подойдет для компаний, работающих с чувствительными данными (персональные данные, данные ограниченного использования, финансовая информация) — как своими, так и их контрагентов.

Суть работы данной программы заключается в том, что сотрудники в офисе или на удаленке, системные администраторы или подрядчики авторизуются через единую точку, которой выступает «СКДПУ НТ Компакт». Система отчетов показывает, кто из пользователей и в какое время находится на IT-инфраструктуре, какие работы проводит. «СКДПУ НТ Компакт» позволяет ограничить совершение потенциально опасных действий и диверсий: запуск запрещенного ПО, изменение настроек серверов, доступ вне разрешенных политик. Если кто-то из пользователей работает во внеурочное время или выполняет подозрительные действия, об этом сообщается в режиме реального времени. В случае если что-то все-таки произошло, все действия сотрудника можно просмотреть через систему в режиме текстовых логов или видеозаписи.

Средства защиты, в том числе и по контролю доступа, недешевы. «СКДПУ НТ Компакт» как раз подойдет тем компаниям, бюджеты которых на информационную безопасность ограничены.

РИСКИ ПАРТНЕРСТВА Самый частотный сценарий кибератак последнего времени — взлом так называемых «цепочек поставок». Исследования говорят о том, что сегодня почти 50% всех утечек из отечественных организаций происходит через контрагентов. Злоумышленники проникают в инфраструктуру небольших компаний, которые оказывают услуги подряда госструктурам или крупным корпорациям и, например, удаленно обновляют ПО на производстве или дорабатывают системы на инфраструктуре заказчика. Через небольшую, плохо защищенную компанию большого гиганта взломать проще, особенно когда уже есть скомпрометированный доступ. Поэтому большим компаниям необходимо в первую очередь задуматься о защите доступов своих подрядчиков. «СКДПУ НТ Компакт» здесь становится той точкой, через которую сотрудник подрядчика входит на инфраструктуру, и все его действия прозрачны. В случае выполнения запрещенных действий сотрудник ИБ-службы получает оповещение, а система отключает нарушителя.

«Но есть и другой аспект таких рабочих отношений,— рассказывает Сергей Бочкарев.— Предположим, вы маленький подрядчик крупного холдинга. И вдруг в инфраструктуре этого холдинга что-то происходит — поломка, утечка. Как доказать, что именно ваша компания ни при чем? Поставить в контур своей организации „СКДПУ НТ Компакт“, через него заходить на инфраструктуру заказчика и самостоятельно записывать все логи и действия своих сотрудников в периметре заказчика. В таком случае вы формируете доказательную „базу невиновности“ перед лицом своего клиента, если у того обнаружены потенциальные угрозы или произошел реальный инцидент. Мы в „АйТи Бастионе“ работаем с нашими заказчиками по такой схеме».

ПРОЗРАЧНЫЙ УДАЛЕНЩИК Хотя тренд на возвращение в офисы после пандемии набирает обороты, огромное число компаний до сих пор работает на удаленке. В IT-компаниях сотрудник на удаленке — это в целом норма, ведь специфика работы в этой сфере позволяет выполнять свои функции из любой точки земного шара. Очень часто такие пользователи обладают повышенными правами, говоря на языке кибербезопасности,— являются привилегированными, суперюзерами. Согласно отчету уже упомянутого „РТК-Солара“, в 60% российских компаний каждый месяц встречаются угрозы привилегированного доступа. Чаще всего суперюзеры скачивают запрещенный контент и обходят политики безопасности в личных целях. Сложнее всего «отловить» проблему пользователей на удаленке. В дистанционном формате в 80% случаев сложнее установить, произошла ли компрометация учетных данных удаленного привилегированного пользователя.

«Контроль удаленного и привилегированного доступов — одна из важнейших проблем для бизнеса сейчас. Собственники привыкли доверять своим сотрудникам, особенно IT-администраторам, но большинство даже не представляет, чем занимается IT-админ, особенно если он на удаленке. Наш продукт „СКДПУ НТ Компакт“ позволяет сделать доступ, с одной стороны, прозрачным, а с другой — контролируемым. Несколько лет назад мы доказывали крупным компаниям, что контроль привилегированного пользователя — это основа кибербезопасности, возможность минимизировать пресловутый „человеческий фактор“. Сейчас крупный бизнес уже понимает это. На очереди — МСБ. Об информационной безопасности нужно задумываться каждому»,— считает господин Бочкарев. ■