Вячеслав Касимов, МКБ: В случае DDoS-атак простои не могут превышать трех минут

В 2024 году финансовый сектор столкнулся с беспрецедентными ковровыми DDoS-атаками. По словам руководителя департамента информационной безопасности МКБ Вячеслава Касимова, возросшие киберугрозы побудили многие банки изменить отношение к DDoS-атакам и переходить на новые решения.

Есть ощущение, что еще лет пять назад DDoS-атаки среди банковских безопасников не считались серьезной угрозой. Но вот на недавнем SOC-форуме эксперты по кибербезопасности говорили о них как о страновой проблеме, о необходимости информационного обмена между банками, защитниками от DDoS, всеми регуляторами, причем не пост-фактум, а непосредственно во время атак. Можно ли говорить о том, что отношение банковской отрасли к этой угрозе поменялось?

Вячеслав Касимов: Да, изменилось. Банковская отрасль осознала, насколько масштабными могут быть DDoS-атаки. Это уже регулярная проблема — редко бывает неделя, когда какой-либо крупный банк не становится жертвой таких атак. Порой это те же группировки, которые повторно атакуют одни и те же банки, особенно если в предыдущий раз организация не смогла эффективно отразить атаку. Это происходит потому, что чем громче информационная волна о недоступности сервисов, тем более успешной считается атака для хактивистов — именно этого они и добиваются. Таким образом, угроза DDoS-атак более чем реальна.

До 2022 года DDoS-атаки, получается, были слабенькие? Или просто это не выходило в публичную плоскость?

Вячеслав Касимов: С одной стороны, они действительно были относительно редкими. С другой — цели таких атак были совершенно иными. Тогда не было стремления сделать атаку резонансной, не было желания опубликовать информацию о том, что какой-то банк недоступен и его клиенты испытывают неудобства. DDoS-атаки в основном носили коммерческий характер: это могли быть конкурентные войны или своего рода месть. Если сейчас взглянуть на архив новостей того времени, сообщения о DDoS-атаках будут появляться от силы дважды в год.

Но все же атаки были. И защита от атак у крупных игроков наверняка была. И вот в начале 2022 года банки, госорганы, ведущие СМИ «легли» под DDoS-атаками. Возникает вопрос, почему?

Вячеслав Касимов: Никто не был готов: не были готовы ни поставщики сервисов, ни поставщики решений, ни потребители. Под «неготовностью» я подразумеваю,

что зачастую решения для защиты от DDoS-атак были либо изначально неэффективными по своей природе, либо были некорректно настроены. На начало 2022 года существовали архитектурные просчеты, а также практически не проводились тренировочные мероприятия. Никто не задумывался, как будет функционировать то или иное решение или сервис, и с каким объемом атак они смогут справиться.

Если говорить о примере «неправильных настроек», то даже если вы приобрели защитный сервис от провайдера, это еще не является гарантией защиты. Нужно правильно настроить логи, наладить схему их отправки и анализировать их. Поставщик должен работать с этими данными, а на основе анализа автоматически включать защиту. Кроме того, анализ занимает некоторое время, и в начале атаки система может быть уязвимой. И, честно говоря, мне кажется, что на момент начала 2022 года многие об этом не задумывались. Именно это и отразилось на тех результатах, которые мы все наблюдаем: многие действительно не выдержали атаки и оказались уязвимыми для более-менее серьезных DDoS.

И как изменился подход в банках, и в МКБ в частности, после событий 2022 года?

Вячеслав Касимов: У нас произошло, можно сказать, идеологическое изменение. Мы больше не работаем с интернет-провайдерами, так как они не справлялись с атаками в начале 2022 года. Теперь мы используем только тех провайдеров, которые предоставляют сервисы очистки трафика вместе с интернет-каналом. Это стало нашей принципиальной позицией.

Кроме того, мы научились грамотно и эффективно передавать логи, делая это правильным образом. С одной стороны, это обеспечивает максимальную прозрачность для сервисов, которые занимаются очисткой трафика, а с другой — мы можем быть уверены, что не передаем какие-либо клиентские данные. Мы также поняли, что одной «чудо-железки», то есть программно-аппаратного комплекса, при серьезной атаке может быть недостаточно — ее нужно будет масштабировать. Однако «чудо-железка» не может сама себя масштабировать. Поэтому мы используем гибридные схемы, которые включают как ПАК, так и возможность подключения облачного сервиса для защиты. В нашем случае это, в том числе, решения российского вендора Servicepipe, которые мы внедрили с помощью ИТ-интегратора «Телеком биржа».

Сложно было найти нового поставщика решений по защите от DDoS-атак?

Вячеслав Касимов: До определенного времени Россия использовала в основном западные решения для защиты от DDoS-атак. Когда иностранные компании-вендоры ушли с рынка, возникла своего рода дилемма: либо платить

повышенную премию для организации параллельного импорта, либо искать альтернативные варианты.

К сожалению, нам требовались специализированные решения, которые не являются продуктами массового рынка, а представляют собой высокопроизводительные системы с сложной внутренней логикой. Например, можно внедрить ПАК — программно-аппаратный комплекс, но его необходимо правильно настроить, чтобы он не становился дополнительной точкой отказа. Ведь через него проходит весь трафик, и если он выйдет из строя, то вся система перестанет работать. Поэтому задача состояла в том, чтобы обеспечить непрерывную работу такого комплекса при любых условиях. Это, конечно же, требует времени и дополнительных усилий.

Почему именно ПАК, они же наверняка дороже? Например, некоторые коллеги из e-com говорят, что у них сервисная модель защиты и им достаточно. Вы говорите, что у вас гибрид — ПАК в составе с ПО от Servicepipe + сервисная модель…

Вячеслав Касимов: Мне кажется, что утверждения о том, что «ПАК не нужен», исходят либо от людей, не совсем понимающих все риски, либо от тех, кто не придает значения конфиденциальности данных своих клиентов и фактически передает эту информацию третьим сторонам — сервис-провайдерам. Когда трафик не идет напрямую в организацию, а проходит через сервис-провайдера, то он имеет доступ ко всей информации, которая передается: от финансовых данных до личных данных клиентов. И только после этого трафик поступает в организацию. Это, конечно, создает дополнительные риски для безопасности и конфиденциальности данных.

Внедряли ли вы защиту от DDoS непосредственно под атакой? Или все всегда было тихо-мирно в спокойном режиме?

Вячеслав Касимов: Было и так. Мы переходили с одного провайдера на другого прямо во время атаки. Это не самая простая и быстрая процедура. Атака происходила на всех уровнях стек-протоколов, а наш сервис-провайдер на тот момент не обеспечивал должную защиту. Поэтому мы сменили провайдера через «Телеком биржу».

Насколько быстро получилось подключить защиту?

Вячеслав Касимов: В нашем случае это произошло быстро, так как мы находились в том же центре обработки данных (ЦОД), что и «Телеком биржа». Нужно было просто провести соединение, а дальше все зависело от скорости работы инженеров ИТ-интегратора, которые занимались установкой этого соединения. В результате нам потребовалось около двух часов.

Как вы оцениваете уровень своей защиты сейчас? Есть ли какие-то целевые показатели, к которым стремитесь? Например, по нормативным актам ЦБ сервисы системно-значимого банка могут быть недоступны до двух часов. Но, мне кажется, что два часа — это очень много….

Вячеслав Касимов: Банк теоретически может оставаться недоступным дольше, но по прошествии двух часов необходимо уведомить регулятора о факте атаки. После этого времени наступает своего рода психологический барьер для Банка России, и регулятор может начать серьезно рассматривать вопрос о внеплановой проверке или введении дополнительных регулирующих мер.

Для самих кредитных организаций ключевые показатели, конечно, другие. Мы, например, договорились с бизнесом, что в случае DDoS-атак простои не могут превышать трех минут. Это важный показатель, который мы использовали при перестройке нашей системы защиты от DDoS.

В целом, проект по модернизации защиты от DDoS мы завершили. Последняя атака, которая была в конце сентября, стала рекордной — 300 гигабит в секунду, а в пике — 310 гигабит в секунду. Мы успешно справились с таким ударом, в том числе благодаря ПАК в составе с ПО DosGate от Servicepipe.

Какие у вас ожидания в части DDOS-атак на 2025 год? Чего стоит ожидать, опасаться кредитным организациям? Может быть, какие-то новые способы нанесения урона и новые тенденции в этой сфере?

Вячеслав Касимов: Прежде всего, стоит опасаться целенаправленных атак со стороны хакерских группировок и киберразведчиков. Если раньше при коммерциализированных атаках основной целью было просто украсть деньги, при этом не нанося серьезного ущерба, то сейчас хактивистыпреследуют множество целей. Если есть возможность украсть деньги — они это сделают. Если можно эксплуатировать конфиденциальную информацию или передать ее третьим лицам — они безусловно это сделают. Если же ни первое, ни второе невозможно, то они наверняка постараются разрушить инфраструктуру.

Ранее были вирусы вроде Petya и NotPetya, которые в принципе предлагали достаточно «честную» сделку: «Если вы не платили за информационную безопасность, то сейчас заплатите выкуп, и мы расшифруем ваши данные». И, как правило, данные действительно расшифровывались. Но теперь, в новых условиях, «честных сделок» уже нет: все зашифруют, и возможности расшифровать не будет. Это очень опасно, потому что, учитывая, что все бизнесы завязаны на работоспособности ИТ-систем, такие действия могут привести к полному краху бизнеса или его длительной остановке.

Что касается DDoS-атак, они никуда не исчезнут и в 2025 году. Хотя принципиально новых видов атак в сфере DDoS, думаю, не стоит ожидать.

Однако недавно я прочитал, что в одном из китайских университетов с помощью квантового компьютера научились взламывать популярные методы шифрования AES и RSA. Эти криптографические методы используются повсеместно, в том числе для формирования электронных подписей в ряде банковских систем. Если это действительно так, то мы можем быть свидетелями революции в области информационной безопасности. Если удастся удешевить работу квантового компьютера, то классическую криптографию можно будет считать взломанной. Но надеюсь, что этого не произойдет.