Облака и ИБ

Издательство: IT-World

Спикер: Иван Мелехин, директор по развитию IZ:SOC компании Информзащита

В настоящее время компании, работающие в области ИБ, и облачные провайдеры находятся на IT-передовой – ведь спрос на их услуги значительно вырос, а трудностей в работе явно не стало меньше. Мы поговорили с участниками этих сегментов IT-рынка о том, с какими проблемами сегодня сталкиваются клиенты, как изменилась динамика кибератак и как защититься от ИБ-угроз при удаленной работе.

Первые проблемы

Алексей САБАНОВ («Аладдин Р.Д.»):

«Одной из насущных проблем является неготовность многих организаций к поддержке защищенного удаленного доступа – не позволяют масштабироваться ни аппаратная, ни программная составляющие. IT-службы не вылезают из ЦОДов и серверных комнат,

многие совершают подвиги, чтобы инфраструктура работала и бизнес-процессы поддерживались на прежнем уровне. Началось секвестирование бюджета, цифры разные, в среднем порядка 20-30%».

Заместитель генерального директора компании «Аладдин Р.Д.» Алексей САБАНОВ отмечает, что особенно тяжело сейчас бюджетным организациям и малому бизнесу. Реалии таковы, что решения надо принимать здесь и сейчас, а планирование бюджета имеет как минимум двухлетний период созревания. Так, для обеспечения полноценного защищенного удаленного доступа на период самоизоляции потребовались срочные закупки аппаратной и программной составляющих, а это смогли позволить себе только организации, способные переправить часть бюджета на срочные нужды.

Г-н Сабанов подчеркивает, что спрос на ноутбуки вырос в марте-апреле в десятки, а то и в сотни раз, чуть ниже был спрос на ПО и средства защиты информации. Сейчас напряжение падает, но проблемы остаются. В частности, выполнение утвержденных планов в условиях самоизоляции усложняется: совещания в онлайн-формате освоили все, но не всегда такой формат может заменить личное общение, деловые встречи. «У малого бизнеса ситуация еще серьезнее, многие компании на грани или уже лишились всего, что было создано до пандемии. Выживают лишь самые сильные и подготовленные, способные адаптироваться к новым условиям. Однако и в этой среде выжившие предприятия все же заботятся о защите удаленного доступа к своим информационным ресурсам», – рассказывает г-н Сабанов.

Никита СЕМЕНОВ (ТАЛМЕР):

«Если раньше предполагалось, что лишь незначительная часть сотрудников будет работать в удаленном режиме, то сейчас клиенты сталкиваются с массовым переходом на удалёнку и, как следствие, понимают, что их системы защиты ориентированы на обеспечение требуемого уровня безопасности лишь в контролируемой зоне, а не за ее пределами».

Руководитель отдела ИБ компании ТАЛМЕР Никита СЕМЕНОВ говорит, что где-то речь идет о банальной нехватке мощностей (например, недостатке лицензий и низкой производительности шлюзов, терминирующих remote access), а где-то это глобальные проблемы отсутствия сертифицированных систем удаленного доступа к чувствительной информации и информационным системам, ее обрабатывающим. Даже крупные клиенты сталкиваются с отсутствием системы видеоконференцсвязи, позволяющей удаленно обсуждать вопросы, касающиеся коммерческой или банковской тайны, отмечает он. В этих условиях одной из важных тем становится защита клиентских устройств – ноутбуков, планшетов и телефонов, домашних компьютеров сотрудников. Сегодня многие работают

на устройствах, о защищенности которых служба ИБ заказчика ничего не знает, считает г-н Семенов. Кроме того, накладываются острые проблемы несовместимости некоторых средств защиты от несанкционированного доступа с носимыми устройствами. «Не все компании имеют EMM- и VDI-решения, рассчитанные на 100% пользователей. Не у всех есть даже достаточное количество лицензированных сессий VPN, ситуация с которыми проще, так как абсолютно все крупные вендоры предоставляют неограниченные лицензии на функционал remote access на период пандемии», – заключает г-н Семенов.

Мурад МУСТАФАЕВ («Онланта»):

«Для заказчиков качество и непрерывность предоставления облачных услуг нашей компанией в текущей ситуации не изменились».

Руководитель службы ИБ компании «Онланта» (входит в группу ЛАНИТ) Мурад МУСТАФАЕВ отмечает, что его компания по-прежнему, даже после перевода всех сотрудников на удаленную работу, соблюдает все регламенты и SLA и прикладывает усилия для поддержания высокого уровня оказания услуг.

Иван Мелехин («ИНФОРМЗАЩИТА»):

«Сейчас, после преодоления первых недель аврала, связанных с массовым переводом сотрудников на удаленную работу, основными сложностями, с которыми сталкиваются наши заказчики, являются задачи по мониторингу киберугроз в этой новой реальности».

Директор SOC АО НИП «Информзащита» Иван МЕЛЕХИН говорит, что старый, хорошо охраняемый периметр безопасности сегодня разрушен, а огромное количество потенциальных точек проникновения вынесено за границу организации. При этом большое количество личных устройств получают доступ к корпоративным ресурсам самыми изощренными способами, тогда как средства защиты, настроенные для контроля потоков, идущих по другим маршрутам, не до конца или вообще не перестроены, в связи с чем появилось множество новых векторов атак. Службам ИБ примерно в таком же авральном режиме, как IT-отделам некоторое время назад, приходится перестраивать схемы защиты под новую реальность.

Владимир УЛЬЯНОВ (Zecurion):

«Самая большая проблема сейчас – борьба с внутренними угрозами. ИБ – это всегда поиск баланса между удобством использования информации и ее защищенностью. С переходом компаний на удаленную работу баланс явно нарушился».

По мнению **руководителя аналитического центра Zecurion Владимира УЛЬЯНОВА,** главный вызов перед ИБ-специалистами сегодня – как сократить риски утечки и при этом сохранить возможность нормально работать. Теоретически можно ужесточить политики использования данных, считает он, но в то же время нельзя оставить без изменений рабочие процессы компаний, которые и так затруднены в связи с тотальным переходом в онлайн.

Георгий МЕГРЕЛИШВИЛИ («СБКлауд»):

«С момента массового перехода компаний на удаленный режим прошел уже месяц, и в целом многие из них вопрос организации такой работы решили. Сейчас на первый план выходит “работа над ошибками”».

Исполнительный директор «СБКлауд» Георгий МЕГРЕЛИШВИЛИ считает, что у компаний уже начался период переосмысления и поиска способов улучшить меры, принятые ранее. В связи с этим о переходе в облако начали задумываться даже те, кто был настроен все решить своими силами. Второй важный вопрос – усложнение поставок оборудования. «Отказ от CAPEX в пользу OPEX весомый аргумент всегда, а в условиях кризиса особенно», – заключает он.

Александр БУРАВЦОВ («Новые Облачные Технологии»):

«В условиях пандемии наши клиенты сталкиваются с необходимостью организации удаленного доступа к своим информационным ресурсам. Им требуется создание новых каналов связи и добавление новых сегментов сети к инфраструктуре компании».

Директор по ИБ «МойОфис» («Новые Облачные Технологии») Александр БУРАВЦОВ говорит, что в процессе организации удаленного доступа уровень безопасности нередко снижается и для всей сети становится равен уровню наиболее слабого звена. В этой связи следует хранить корпоративные данные в защищенном периметре организации и обеспечивать максимальный уровень их безопасности. «Наши клиенты, использующие платформу “МойОфис”, в которую заложена концепция частного облака, успешно преодолевают эти трудности», – отмечает г-н Буравцов.

Василий СТЕПАНЕНКО (DataLine):

«IT-службы некоторых компаний оказались не готовы к организации удаленной работы сотрудников в период самоизоляции. Не всегда помогает даже то, что многие вендоры предоставляют бесплатные VPN-клиенты на период пандемии, так как не всегда в штате имеются квалифицированные инженеры, способные все правильно настроить».

По словам директора центра киберзащиты DataLine Василия СТЕПАНЕНКО, некоторые сотрудники оказались не готовы работать удаленно: не у всех дома есть соответствующие требованиям ПК. Отсутствие инструкций по подключению к корпоративной сети вызвало шквал запросов в техподдержки, с которыми удалось окончательно справиться только спустя пару недель. Как утверждает г-н Степаненко, решения класса NAC (Network Access Control) практически не используются, в связи с чем не проводится проверка личных устройств сотрудников на соответствие требованиям ИБ (наличие обновленного антивируса, ОС со всеми обновлениями, разграничение прав и пр.), в результате появляется возможность заражения корпоративных ресурсов клиентов. Кроме того, мало кто использует двухфакторную аутентификацию и CAPTCHA, и злоумышленники получают шанс на успешные переборы паролей к доступным корпоративным ресурсам из Интернета, например OWA (Outlook Web Access), предупреждает г-н Степаненко.

Удалёнка и кибератаки

Увеличилось ли число кибератак на компании в связи с ростом объемов их удаленной деятельности? Если да, то каких именно и в каких масштабах?

Алексей САБАНОВ («Аладдин Р.Д.»):

«О серьезном увеличении числа кибератак не слышал. Стабильный их рост за последние годы имеет флуктуации, если отклонения и есть, они пока в пределах этих флуктуаций».

Никита СЕМЕНОВ (ТАЛМЕР):

«Число кибератак увеличилось ощутимо, однако качество и степень их проработанности резко снизились. В основном мы наблюдаем всплеск простейших фишинговых рассылок, спама и botnet-активности. Возможно, это подготовка к чему-то большему, однако скорее похоже на действия низкоквалифицированных злоумышленников».

Никита СЕМЕНОВ (ТАЛМЕР) убежден, что из всего списка наибольшего внимания заслуживают botnet-активности, которые могут остаться незамеченными из-за перехода на удаленную работу, особенно если у клиента не развернуты специализированные средства защиты – anti-botnet и IPS.

Мурад МУСТАФАЕВ («Онланта»):

«В марте среднее количество заблокированных атак составило 112 тысяч. А в апреле – 142 тысячи, что примерно на 30% больше».

Мурад МУСТАФАЕВ («Онланта») уверен, что злоумышленники ведут свою работу непрерывно. Но такой небольшой рост атак оборудование и сеть компании выдерживают легко, поэтому это никак не отразилось на предоставляемых клиентам услугах.

Иван МЕЛЕХИН («Информзащита»):

«В условиях удаленной работы в первую очередь выросло количество фишинговых атак, которые эксплуатируют тему коронавируса».

Иван МЕЛЕХИН («Информзащита») также отмечает рост попыток проникновения в корпоративные сети через вновь организованные точки доступа – VPN-шлюзы, терминальные серверы. «Количество наблюдаемых нашим SOC событий типа компрометации актива выросло по сравнению с январем 2020 года на 48%, а связанных с вредоносным ПО – на 20%», – уточняет он.

Владимир УЛЬЯНОВ (Zecurion):

«Количество атак заметно увеличилось, но не всяких, а именно инсайдерских, со стороны собственных сотрудников компаний. В марте наш аналитический центр предсказывал рост утечек конфиденциальных данных в два-три раза в связи с переходом компаний на удалёнку, и сейчас мы можем говорить, что прогноз оправдался».

Владимир УЛЬЯНОВ (Zecurion) полагает, что причин для роста инсайдерских атак немало: снижение лояльности, неуверенность в завтрашнем дне, стремление перестраховаться и скопировать информацию «на всякий случай», уменьшение страха перед нарушением, если оно будет выявлено службой безопасности (ведь она физически находится где-то далеко и всегда можно успеть что-нибудь придумать). К этому можно добавить участившиеся случаи переманивания кадров, вербовки инсайдеров конкурентами и злоумышленниками, повышенную уязвимость перед методами социальной инженерии. Фактически речь идет о том, что люди стараются компенсировать снижение доходов за счет работодателя, считает г-н Ульянов.

Георгий МЕГРЕЛИШВИЛИ («СБКлауд»):

«Наши партнеры в сфере ИБ отмечают возросшее число атак на сети “домашних” провайдеров, так как в них переместился значительный объем корпоративного трафика. Это повод задуматься о дополнительной защите VPN-каналов и личных устройств, которые сотрудники используют для рабочих задач».

Александр БУРАВЦОВ («Новые Облачные Технологии»):

«Работа из дома объективно увеличивает риски утечки корпоративных данных. Компании приходится учитывать факты использования личных компьютеров, теперь сложнее контролировать устанавливаемое ПО, переход на вредоносные веб-ресурсы или выход в Сеть через незащищенные соединения».

Александр БУРАВЦОВ («Новые Облачные Технологии») приводит итоги исследования, проведенного «Лабораторией Касперского» задолго до пандемии: 62% владельцев компаний и их сотрудников используют личные устройства для работы, причем 92% из них хранят важные корпоративные данные на своих смартфонах и планшетах. В условиях удаленной работы эти показатели будут еще выше, считает он, и напоминает, что не менее 30% атак совершается в результате установки вредоносных программ. Угрозу также несут небезопасные сети Wi-Fi и открытое хранение ключей доступа. «Новым направлением кибератак, которое активно растет в период пандемии,

стали домашние “умные” устройства — на них часто не меняют заводские пароли», – говорит он.

Василий СТЕПАНЕНКО (DataLine) подтверждает, что ряд клиентов его компании столкнулся с фишинговыми атаками, много заражений серверов вредоносным ПО с целью осуществления незаконной деятельности, в том числе DDoS-атак. «Мы узнаем о таких фактах по жалобам на IP-адреса, которые принадлежат нам и сдаются в аренду клиентам. Сами же клиенты редко делятся такой информацией, а у тех, у кого мы администрируем средства защиты, особых всплесков на сегодняшний день не отмечено. Статистика практически такая же, как и до самоизоляции, даже у ретейла», – поясняет он. Чаще всего жалобы приходят от таких ресурсов, как @spamhaus.org, @netcraft.com, @bitninja.io, @blocklist.de, spamcop.net, NiX Spam, botnet.tracker. Пользуясь случаем, г-н Степаненко передает им благодарность за работу.