Эволюция высоких технологий: переход из тени на главную роль

В 2020 г. организации повсеместно стали переводить своих сотрудников на удаленную работу, все больше людей оказались запертыми дома из-за карантина. В этих условиях **ИТ-инфраструктура стала в один ряд с такими важнейшими коммунальными услугами, как водо-, газо- и электроснабжение**. Без подключения к сетям связи, телекоммуникационным сервисам и облачным хранилищам многие организации просто не могут работать, а потребители будет существенно ограничены в возможности приобретения необходимых товаров, общении и развлечениях. Супермаркеты, вещатели, операторы финансовых услуг и многие другие компании смогли продолжить работу исключительно благодаря развитым информационным технологиям.

Онлайн-покупки — особенно в отношении товаров первой необходимости — стали обыденным делом, а **мировой сетевой трафик в этом сегменте вырос более чем на треть**. Подписки на стриминговые сервисы бьют все рекорды — к концу июня Netflix приобрел 26 млн новых подписчиков. Количество пользователей соцсетей, мессенджеров и платформ видеосвязи также выросло. Самые впечатляющие результаты продемонстрировала **платформа Zoom: рост выручки по сравнению с 2019 г. составил 335%**. Сегодня практически все в нашей жизни, от медицинских консультаций или проверки банковского счета и до занятий спортом подчинено

принципам digital-first. Так что же изменится с переходом ИТ из разряда второстепенных услуг в статус одной из ключевых инфраструктур? Последствия для технологической отрасли сложно переоценить. Роль и ценность информационных технологий для экономики и общества сегодня очевидна для всех. Безусловно, для провайдеров SaaS, облачных и сетевых сервисов это отличные новости, однако большое влияние — это и большая ответственность.

Отключения недопустимы

Коль скоро ИТ переходит в разряд критически важной инфраструктуры, необходимо обеспечить постоянную доступность ресурсов. Задумайтесь: как часто случаются перебои с подачей воды или электричества? Случаются они крайне редко, всякий раз вызывают бурную общественную реакцию и попадают в главные новости. Можем ли мы утверждать, что доступность ИТ-сервисов находится на таком же уровне? Как часто приходится перезагружать роутеры, а приложения перестают реагировать на команды? Более того, постоянно происходят кибератаки с утечкой данных: согласно некоторым исследованиям **ежедневно взламывается до 30 000 веб-сайтов**. Если уж технологические сервисы действительно переходят в разряд ключевых инфраструктур, необходимо обеспечить определенные стандарты качества обслуживания, согласно которым **операторы будут нести ответственность перед независимыми регуляторами**. Проще говоря, такие ситуации как «невозможно отобразить страницу» или «компьютер не отвечает» должны уйти в прошлое. И хотя технологическим гигантам такой поворот может нравиться, это — одно из ключевых требований в свете того, насколько важную роль информационные технологии играют сегодня практически во всех аспектах нашей жизни.

Впрочем, помимо возможного сопротивления со стороны Кремниевой долины, говоря о регулировании технологического сектора, следует рассмотреть и другие риски. Например, если речь идет о социальных сетях и поисковых сервисах, то возникает беспрецедентная ситуация, когда **требование об обеспечении определенного уровня обслуживания выдвигается в отношении услуг, за которые потребитель не платит**. С другой стороны, **подписные модели SaaS вполне соответствуют такому регулированию**. В принципе, такой вариант регулирования уже существует на рынке в виде «Соглашения об уровне обслуживания» (Service License Agreement, SLA). Оно формируется поставщиком услуг или сервисов, и после заключения договора с партнером или клиентом поставщик обязан выполнять его условия. Учитывая, что простои и недоступность ресурсов влекут за собой значительный ущерб для бизнеса, клиенты предъявляют к поставщикам все более высокие требования.

Согласно Отчету Veeam о тенденциях в области защиты данных за 2020 г., 95% организаций по всему миру сталкивались с непрогнозируемыми сбоями или отказами ИТ-систем. Средняя продолжительность простоя составила почти 2 часа. Убытки из-за перебоев в функционировании критически важных приложений — а такие приложения обычно составляют более половины от всех, используемых организацией — в среднем оцениваются в $67 651 в час. Это означает, что в каждой такой ситуации, когда организация не может использовать электронную почту, платежные инструменты, веб-сайты или

мобильные приложения, общий ущерб в среднем превышает $135 000. И хотя в каждом конкретном случае компании могут требовать компенсации убытков, менять поставщиков услуг, если они не обеспечивают должный уровень обслуживания, или требовать внепланового ремонта оборудования, вызывающего сбои, не существует универсального решения, позволяющего защитить бизнес. Один из шагов на пути к более жесткому регулированию технологических и телеком-компаний — **формирование минимальных требований к уровню обслуживания, включая ограничение максимального допустимого времени простоя, време**ни на восстановление данных и приложений, частоты обновлений ПО.

Сохранение репутации высоких технологий

Говоря о сбоях, простоях и прочих неполадках, подрывающих статус ИТ как базовой инфраструктуры, обязательно стоит уделить внимание кибербезопасности. Растущее значение ИТ для повседневного функционирования современного мира открывает для киберпреступников новые возможности, которые они обязательно постараются использовать. **Все, что подключено к сети, может быть взломано**. И что же будет с миром, где к сети подключено вообще все? В 2020 году количество кибератак опять выросло. Отчет Microsoft Digital Defense за 2020 год показывает, что в этот период один только Office 365 заблокировал более 1,6 млрд фишинговых гиперссылок в электронных письмах. Всего **на вирусы было просканировано 6 трлн писем и 13 млрд из них были заблокированы, поскольку являлись вредоносными**. Эта информация соответствует данным собственного исследования Veeam, в котором ИТ-руководители назвали киберугрозы основной проблемой следующего года и поставили их выше таких проблем как недостаток нужных компетенций у сотрудников и удовлетворение требований пользователей.

При этом организации, которые не позаботились о безопасности своих ИТ-систем, уже сейчас могут очень сильно пострадать. Финансовые убытки по причине сбоев и простоев, потеря доверия клиентов и репутационный ущерб — негативные последствия могут быть настолько велики, что компания уже не сможет оправиться от них. Это еще раз подчеркивает **важный статус технологической инфраструктуры** — только на сей раз в том, что касается кибербезопасности и защиты данных. Возможно, следует поменять подход к оценке: важно не то, какой поставщик решений безопасности обслуживает организацию, а то, какие протоколы безопасности организация должна внедрить у себя, исходя из того, с какими данными она работает. Общий регламент ЕС о защите данных (GDPR), действующий в отношении персональных данных граждан ЕС, в определенной степени способствует внедрению универсальной системы регулирования. Однако пока внедрение систем киберзащиты определяется собственными решениями организации, а не является исполнением обязательных требований. Если статус вопросов кибербезопасности меняется, и из «одного из компонентов ИТ, внедряемых на усмотрение организаций» они становятся обязательным компонентом инфраструктуры, то это дает возможность распространить лучшие отраслевые практики на весь рынок. **Станет ли обучение в области кибербезопасности обязательным для офисных сотрудников**, особенно с учетом роста количества удаленных работников? Должны ли все организации публиковать

полноценный план аварийного восстановления с подробным указанием, как именно они будут восстанавливать данные в случае их кражи или утраты? Более того, должно ли хранение личных данных граждан в организации подчиняться универсальному стандарту в части кибербезопасности, который будет гарантировать необходимый уровень их защиты?

Тенденции проникновения информационных технологий во все сферы нашей рабочей и личной жизни — как и непрекращающееся противостояние организаций и киберпреступников — возникли задолго до 2020 г. Однако этот год несомненно стал переломным в вопросе восприятия информационных технологий и в том, что отрасли пора продемонстрировать свое ответственное отношение. Мы уже стали свидетелями общественного порицания компаний, которые не принимают должных мер для защиты информации или используют данные неэтично. При этом и руководители компаний, и обычные люди по всему миру осознали, что постоянный доступ в интернет уже стал необходимой частью обычной жизни. Возможность общаться, обмениваться контентом и совершать сделки через сеть обогащает нашу экономику, наше общество, нашу жизнь. Роль технологий в мире изменилась: теперь само собой разумеется, что они доступны постоянно и повсеместно. Мир просто не готов больше мириться с сообщением «Не удается отобразить страницу».

Дэйв РАССЕЛ,

вице-президент Veeam по корпоративной стратегии

https://www.it-world.ru/it-news/reviews/157721.html