Опыт Lenvendo по поддержке ИТ-инфраструктуры в условиях санкций

**22 сентября прошел вебинар «Как обеспечить непрерывность работы ИТ и ИТ-инфраструктуры. Полгода в режиме турбулентности». В онлайн-мероприятии принял участие руководитель отдела SRE и DevOps компании Lenvendo Владислав Карпенков.**

Состоялся второе онлайн-мероприятие из серии «Как обеспечить непрерывность работы ИТ и ИТ-инфраструктуры. Полгода в режиме турбулентности», организованное компанией M1Cloud. Серия вебинаров направлена на обмен актуальной информацией и мнениями между ИТ-директорам, руководителями профильных отделов из компаний среднего и крупного бизнеса, а также собственников предприятий, заинтересованным в развитии ИТ-направления.

Прошедшее мероприятие собрало более 70 слушателей. В онлайн-режиме они получили ответы на наболевшие вопросы от профильных экспертов обсудили пути решения возникших и возможных проблем, чтобы обеспечить стабильное функционирование отечественной ИТ-индустрии для бесперебойной работы бизнеса.

В мероприятии приняли участие директор по архитектуре ИТ S7 Дмитрий Носивской, директор по развитию бизнеса Stack Group Владимир Лебедев, руководитель отдела архитектуры клиентских решений M1Cloud Алексей Воробьев и Владислав Карпенков, руководитель отдела SRE и DevOps компании Lenvendo. Он выступили докладом на тему «Изменения работы ИТ в сфере разработки и поддержки Highload-проектов в период санкций. Опыт компании Lenvendo» выступил. В прямом эфире он поделился антикризисными мерами для обеспечения непрерывности бизнес-процессов и актуальными методами противостояния DDoS-атакам.

**Как изменилась поддержка ИТ-инфраструктуры за последние полгода?**

Владислав отметил, что в марте большинство компаний столкнулись с необходимостью частичной трансформации или глобальной перестройки ИТ-инфраструктуры. В частности, закупить «железо» стало значительно сложнее: привычный ассортимент уменьшился, цены выросли, а новые цепочки поставок еще не стабилизировались. Одним из основных выходов Владислав считает переход на облачные решения. Благодаря такому подходу заказчик делегирует ответственность за корректную работу инфраструктуры и хранение данных компании, а также избавляется от затрат на обслуживание серверов.

**Доступные Open Source-продукты**

В рамках доклада также обсудили какими Open Source-решениями можно заменить ПО недоступное в России. К примеру, альтернативой Slack и Microsoft Teams может стать Mattermost — внутрикорпоративный онлайн-чат с открытым кодом и возможностью обмена файлами, поиска и интеграции.

Альтернативой Veeam Software и других платных систем копирования может выступить Bareos — cетевое кроссплатформенное ПО для резервного копирования, архивирования и восстановления данных, которое уже давно применяется специалистами Lenvendo.

**Что может помочь предотвратить DDoS-атаки?**

В качестве одного из основных маркеров последнего полугодия был отмечен повышенный интерес киберпреступников на RU-сегмент. DDoS-атакам регулярно подвергаются сайты и бизнес-приложения компаний вне зависимости от их масштаба и политической ангажированности.

Для компаний, которые могут позволить существенные и регулярные расходы на организацию кибербезопасности Владислав Карпенков порекомендовал обратиться к решениям Qrator и Kaspersky.

Для тех, кто не готов к существенному финансированию этого направления тоже есть рекомендации:

1. Если клиенты сайта или бизнес-приложения локализованы только в России можно отфильтровать трафик на уровне nginx с модулем GeoIP2. Такое решение по понятным причинам нестабильно работает в Крыму, нетривиально в настройке и обслуживании, также некоторые системы маркетплейс или иные интеграции могут попасть под блокировки.
2. Если нет большого количества интеграций с разными маркетплейс и иными сервисами или все интеграции известны заранее, а сайт не должен быть индексируемым можно фильтровать HTTP 1.1 и использовать только HTTP 2.0. Такое решение существенно снижает вредоносный трафик, но с большой долей вероятности перестанет работать индексирование, интеграции и другие сервисы, которые в силу «возраста» не умеют HTTP 2.0. Оптимально для корпоративных порталов.
3. Включите ограничения rate/limit/burst. При этом методе специалисты отмечают простую реализацию и стабильную работу решения, но необходимо время на калибровку и адаптацию параметров ограничения и возможны отключения релевантного трафика.

Как вы видите, у всех методик есть свои плюсы и минусы. Несомненно, также и то, что каждая система уникальна, а от объема инфраструктуры и поставленных задач будет зависеть механики работ и перечень использованных продуктов. Если вам необходима консультация по оптимизации или поддержке ИТ-инфраструктуры – вы всегда можете обратиться к нашим специалистам на info@lenvendo.ru