В свете последних событий и беспрецедентного увеличения количества атак на инфраструктуру, специалисты «Код безопасности» настоятельно рекомендуют, для пользователей продукции VMware обратить внимание на следующие настройки для хостов виртуализации и управляющего центра:

-произвести аудит парольной политики и обновление паролей, при подозрении на компрометацию данных (как извне, так и со стороны внутренних или наёмных сотрудников организации)

-активировать и настроить встроенный фаервол

-убедиться, что запрещён прямой доступ в интернет к web-интерфейсу хостами и управляющим центром из интернета

-убедиться, что запрещён прямой доступ к службе ssh из интернета (либо, если это невозможно, доступ к SSH осуществляется с использованием сертификатов безопасности, но не пароля)

-для доступа к объектам виртуализации из сети Интернет, желательно настроить и использовать, средства криптографической защиты, jump серверы и т.п.

-настроить ролевую модель доступа, а также, обязательно провести аудит существующей – проверить отсутствие неизвестных учётных записей, и УЗ уволенных сотрудников. Провести аудит и убрать избыточные права у существующих пользователей

-обеспечить передачу журналов событий, в сторонние системы с возможностью мониторинга и оповещения администраторов о подозрительных событиях

-ограничить использование ESXi-shell и интерфейса DCUI на хостах виртуализации

-ограничить использование внешний USB-устройств для хостов виртуализации (особенно, если они располагаются в западных дата-центрах)

-обеспечить разделение management-сети, сетей пользователей и репликации/резервного копирования данных

-при необходимости обеспечить сегментацию для виртуальных машин, работающих в рамках одного хоста или кластера хостов

Для пользователей СЗИ от НСД vGate – проверить, что ПО переведено в штатный режим работы, доступ к серверам виртуализации имеют только аутентифицированные в vGate пользователи, провести аудит имеющихся правил разграничения доступа, а так же настроек и назначения политик безопасности, убедиться, что настроены сервер мониторинга и правила корреляции событий (с обязательным отображением действий в обход vGate), убедиться, что настроены правила микросегментации для виртуальных машин.