Уважаемые клиенты!

В последнее время участились случаи не санкционированного доступа к сетевым видеорегистраторам с последующей их блокировкой. В связи с этим наша компания настоятельно рекомендует Вам выполнить следующие действия для предотвращения несанкционированного доступа к вашим сетевым видеорегистраторам и видеокамерам:

1. Смена заводского пароля на личный, используя при этом и цифры и буквы.
2. Без острой необходимости не подключать видеорегистратор к локальной сети, либо к интернету.
3. Не записывать логин и пароль от регистратора на нем либо другом видном месте.
4. Использовать не стандартную подсеть при настройке регистратора(к примеру 192.168.55.*, стандартными сетями считаются 192.168.0.*,192.168.1.*).
5. Физически разделить сети. Не использовать текущую компьютерную сеть в которую включены офисные компьютеры, что бы предотвратить доступ сторонних лиц.
6. Если нет возможности физически разнести сети то использовать на коммутаторах настройку Vlan.
7. Не стоит разглашать IP адрес и маску как регистратора, так и сети в целом.
8. Настроить на самом регистраторе черные и белые списки ip адресов, имеющих доступ к регистратору.
9. Скрыть место установки видеорегистратора.
10. Так же безопасность может повысить правильная настройка роутера (в роутерах встроен брэндмауер, настройка доступа(черные и белые списки ip адресов)).
11. Контролирующему персоналу выдавать доступ только через CMS, а не web-интерфейс, т.к. при доступе через web-интерфейс контролер будет иметь доступ ко всем настройкам регистратора.

Благодарим Вас за внимание.