Сервисный центр должен не только чинить, но и заботиться о безопасности

Вопросы кибербезопасности далеко не всегда связаны с угрозами в виде абстрактных хакеров, ежедневно взламывающими сервера Пентагона перед завтраком. Как правило, в большинстве случаев, всё гораздо проще и скучнее. Но когда вместо состязания интеллектов IT-специалистов, причиной взлома становится разгильдяйство, финальный результат оказывается куда как разрушительней.

Например, IP-камера видеонаблюдения. Наверное, её можно пытаться взломать и хакерскими методами, но зачем так напрягаться, когда достаточно найти возможность сбросить пароль для входа в систему управления камерой? А для этого, достаточно найти сервисный центр, авторизованный для обслуживания данного вида камер, и попросить помочь с восстановлением пароля. Дальше, всё просто. Если работа в сервисном центре поставлена плохо, со сбросом пароля просто так, без лишних телодвижений, могут и помочь. И тогда однажды, камеры этого вида на любом предприятии могут оказаться под контролем злоумышленников.

Поэтому в организациях, где заботятся о безопасности своих клиентов, помощь в сбросе паролей оказывается только при наличии доказательств, что камера принадлежит именно тому лицу, которое обращается с просьбой.

Например, в сервисном центре НАГ предлагают два варианта подтверждения владения камерой.

Если камера куплена легально, и все документы в наличии, надо выполнить несложную инструкцию, заполнить шаблон и отправить его специалистам. В ответ, клиенту будет выслан сервисный пароль. Если документов не сохранилось, можно просто саму камеру отправить в СЦ и уже там специалисты произведут сброс пароля. Эта процедура по факту защищает камеру и регистратор от попытки взлома, даже если у злоумышленников имеется к ней физический доступ: ведь в этом случае камеру придётся демонтировать на приличное время, что незаметно сделать весьма проблематично. Кроме того, по факту оплаты услуг, в сервисном центре останутся реквизиты плательщика.

Все прочие варианты не рассматриваются, даже под угрозой недовольства настоящих клиентов, которым лень выполнять положения инструкции. Безопасность важнее.

Типовым примером, когда это правило помешает злоумышленникам, можно считать желание сотрудника предприятия что-то незаметно стереть в записях. Документов на камеру наблюдения у него нет, демонтировать и отправить её в СЦ, с последующей оплатой услуг, он разумеется, тоже не может. Таким образом, простым правилом отсекается целый пласт злоупотреблений при физическом доступе к камере.

Но не всем это нравится. Вот текст реального обращения в сервисный центр НАГ в ответ на отказ предоставить данные для сброса пароля под "честное пионерское" (стилистика и орфография оригинала сохранены):

> *Осталось очень неприятное впечатление от вашей компании.*
> *Стоят у нас несколько видеокамер OMNY, кто ставил теперь не найти и пароли тоже.*
> *"Наш внутренний регламент запрещает предоставлять услугу сброса пароля удаленно без документов на приобретение."*
> *Отлично, проще выкинуть ваше оборудование и поставить кого нибудь "попроще", я с ХИКом не имел таких проблем.*
> *Они лучше относятся к своим потребителям с ними проще договориться.*

В ситуации "с ними проще договориться" надо понимать, что эта "простота" может однажды повернуться и против самого клиента, если с СЦ вендора "договорится" конкурент или злоумышленник. Или, к примеру, на предприятии готовится хищение имущества (или другие тёмные делишки), и в качестве "договаривающейся" стороны может выступить злодей из числа собственных сотрудников, вполне официально в организации работающий, но никакого отношения к обеспечению безопасности, не имеющий.

Специалисты в НАГ вполне адекватны и прекрасно понимают, как в отечественных реалиях на территории любого предприятия может работать настоящий "зоопарк" из камер наблюдения, данные для управления которыми, утеряны. И вполне допускают, что к ним обращается настоящий владелец камер OMNY, благо они довольно популярны и достаточно распространены. Но предоставлять по любому запросу сведения, которые могут поставить под удар интересы клиента – категорически нельзя. Все действия специалистов в СЦ, так или иначе связанные с безопасностью, тщательно регламентированы и жёстко контролируются.

Ситуаций, при которых стороннее лицо может хотеть получить доступ к чужой камере, довольно много. От хулиганства и нежелания платить абонентскую плату за использование до выведывания коммерческих тайн или банального грабежа. Сервисный центр не может превращаться в источник угрозы для своих клиентов.

И чем больше сервисных центров будет следовать этой нехитрой логике, тем лучше будет для всех.