КАК ПОСТРОИТЬ «УМНЫЙ» БЕЗОПАСНЫЙ ДОМ?

Представьте будущее, как в фантастических фильмах с летающими автомобилями, человекоподобными роботами-помощниками, работающими людьми 60+ и непременным атрибутом — «умным домом». Почти таким же умным, как в пыльном рассказе Рэя Брэдбери «Будет ласковый дождь», где «умный дом» продолжал жить без своих хозяев, выполняя повседневные обязанности, вроде приготовления завтрака. И если до летающих автомобилей человек все еще безумно далек, то «умный дом» это уже продукт сегодняшнего дня.

В нынешних реалиях понятие «умный дом» — система домашних устройств, способных выполнять действия и решать определенные повседневные задачи без участия человека. Человек всегда старался сделать свое жилье максимально комфортным и безопасным, а Ростелеком дает осуществить такую возможность благодаря собственному продукту «Умный дом».

Свет по команде в любом цветовом диапазоне, когда вы заходите в квартиру, а также в отсутствие хозяев для имитации деятельности в пустом доме при наступлении темноты — пожалуйста. Забыли выключить опасный электроприбор, например, утюг? Отключите его одним нажатием кнопки на смартфоне. Или подогрейте воду в чайнике пока едете домой по пробкам. Датчик открытия позволит узнать, куда пропадают спрятанные в шкафу конфеты, когда родителей нет дома. Датчики протечки вовремя оповестят о внезапном прорыве шланга стиральной машины, а другие даже смогут перекрыть воду. Помимо прочего возможен контроль водосчетчиков и снятие с них данных не только о количестве потребляемой воды, но также и ее температуре. И в случае если вода не соответствует нормативам нагрева, у владельца будет неоспоримый аргумент для перерасчета. «Умный дом» оповестит о «внезапных гостях» в ваше отсутствие, напомнит о незакрытых дверях и окнах. Мгновенно среагирует на появление дыма или газа звуковым сигналом, push-уведомлением и сообщением на телефон. И, конечно же, главный атрибут безопасности — услуга видеонаблюдения, в которой доступны прямые трансляции на мобильный телефон или веб-кабинет, хранение записей на протяжении семи дней, отслеживание видеоаналитики: движение в кадре, перекрытие обзора, отключение камеры, отправка уведомлений, сохранение скриншотов и роликов в формате mp4. Помимо прочего есть возможность прописать различные сценарии на взаимодействие нескольких приборов.

Ростелеком предлагает два комплекта «Умного дома»: расширенный и базовый. Базовый включает в себя контроллер с протоколом Z-Wave Plus, датчики открытия, движения. Расширенный комплект дополняется датчиками дыма и протечки.

И это только готовые предложения. Контроллер от Ростелекома позволяет подключить к нему более двух сотен устройств, которые вы только сможете найти на рынке предложений для «умных домов». Инфракрасный датчик превратит смартфон в универсальный пульт от любого электроприбора с пультом в доме. Датчики проникновения и движения могут просто не среагировать на злоумышленников уведомлением, а можно добавить к ним оглушающую сирену. Датчики управления шторами, светом, умные розетки с подключенными обогревателями, кондиционерами или кухонными вытяжками и всего, что только можно придумать в связке с датчиками температуры, влажности, освещенности и другими показателями, могут полностью автоматизировать рутинные процессы, обогреть, проветрить, увлажнить и вообще добиться комфортной и приятной атмосферы в доме, не прилагая никаких самостоятельных усилий. Способы применения и сценарии ограничены только фантазией хозяина жилища. Скорее всего, это и есть будущее, хоть и без летающих автомобилей, но хотя бы у себя дома.

Источник: ***www.respnews.ru***

ЧЕМ МОЖЕТ БЫТЬ ОПАСЕН «УМНЫЙ ДОМ»

«Умный дом» — целая система, делающая жизнь хозяина проще и комфортнее. Люди наконец-то могут лежа в постели управлять домом так, как это смог бы сделать обслуживающий персонал из нескольких человек. Казалось бы, как «умный дом» может принести прямо противоположный эффект?

В положительном ключе «умный дом» наоборот может обезопасить дом. Так, имея «умный дом» в Подмосковье и находясь в Мюнхене, вы можете с помощью смартфона или планшета, имеющего выход в Интернет, управлять своим местом проживания.

Без вашего участия продвинутые системы могут предотвращать ЧП, например, короткое замыкание или затопление. Естественно, такого помощника и охранника сложно представить вредоносным. Тем не менее, ничего в мире идеального нет, и «умный дом» не является исключением.

«Умным домом», как и любой техникой, всегда что-то управляет. В этом случае управленцем является центральный сервер. Это некий компьютер, адаптированный специально под эту систему, имеет повышенную защиту и узкую направленность. Его главным отличием является программное обеспечение. А оно, как и все программы, имеет свои уязвимости. По сути, его можно заразить особенной вредоносной программой, как и ваш обычный настольный компьютер.

Как правило, современные системы подключены к Интернету, что и является проводником для злоумышленников. Человек, имеющий определенный навык во взломах, сможет получить доступ к серверу, управляющему «умным домом» в обход файерволла и брандмауэра. Альтернативой может стать использование уязвимостей мобильного устройства (если вы управляете «умным домом» удаленно) для взлома сервера.

Среди таких систем есть и более защищенные, подключающиеся к сети на определенное время. Сеансы подключения обычно занимают непродолжительное время, что значительно усложняет взлом системы.

Злоумышленник может быть уже на полпути к успеху, но если сеанс подключения будет завершен, а подключение сброшено, то ему придется начинать все сначала. Вместе с этим используются и улучшенные брандмауэры, ключи шифрования со сложной технологией и VPN.

Естественно, если у системы отсутствует подключение к сети, то взломать такую систему практически не представляется возможным. Однако это неудобно для самого хозяина, поскольку такой «умный дом» не совсем-то и умный, и выполняет только часть потенциальных возможностей.

Как вы уже знаете, «умный дом» состоит из сервера, а также сенсоров. В большинстве случаев сенсоры подключаются к серверу по Wi-Fi, либо по Bluetooth, поскольку это избавляет от необходимости проводить множество проводов.

Вместе с этим, беспроводное соединение более уязвимо к атаке и взлому. Протоколы шифрования, использующиеся в Wi-Fi, очень слабы, что позволяет даже горе-хакеру получить несанкционированный доступ к системе.

Взломав такую систему, злоумышленник может получить доступ сразу ко всем компонентам управления, например, открыть беспроводной замок, получить съемку камер наблюдения. Сильно постаравшись можно даже умышленно создать аварийную ситуацию.

Обезопасить использование системы можно, следуя некоторым правилам. Пользуйтесь прерываемыми сеансами подключения к Интернету, установите глушители беспроводных сетей Wi-Fi или Bluetooth вне дома, где сеть еще присутствует, либо вообще откажитесь от беспроводного соединения модулей.

Помните, что несоблюдение элементарных правил безопасности не только не сделает использование системы «умный дом» действительно комфортной, но и может привести к диаметрально противоположным результатам.

Источник: ***www.ingsvd.ru***

КАК ВЕЩИ СХОДЯТ С УМА ИЗ-ЗА ИНТЕРНЕТ-ЗАВИСИМОСТИ

Представьте: вы торопитесь домой после утомительного рабочего дня. Открываете приложение на смартфоне, касаетесь кнопки на экране — и тут же в десятке километрах от вас оживает ваша квартира. Загораются «умные» лампочки, «умный» термостат начинает нагревать помещение, «умный» чайник кипятит воду для вечернего чаепития. Удобная штука «умный дом»!

Но у каждой медали две стороны, и на оборотной стороне этой — зависимость «умных домов» от работоспособности многих других вещей. Выйти из строя может любой компонент системы, и чем больше в ней сторонних продуктов, тем меньше стоит рассчитывать на ее надежность.

В холодном плену

Недавно Twitter захлестнула волна жалоб: пользователи термостатов Netatmo писали, что внезапно потеряли возможность контролировать температуру в своих домах. Оказалось, что несколько серверов Netatmo упали, а оставшиеся не смогли справиться с нагрузкой и обработать запросы всех пользователей.

На этот случай в термостатах Netatmo предусмотрен режим ручного управления, который позволяет изменить температуру вручную, без приложения. Но, по всей видимости, у некоторых пользователей этот режим просто не работал, поэтому они вынуждены были дрожать от холода, любуясь на гениальное, но полностью бесполезное достижение техники.

Зависимость от сторонних поставщиков дополнительно повышает вероятность сбоев, и проблема ненадежности встает еще острее. Например, некоторые гаджеты для продвинутых домов управляются через весьма занятный сервис под названием

IFTTT (If This Then That, что можно примерно перевести как «Если произойдет это, сделать то»), размещенный на платформе Amazon Web Services. В прошлом году серверы IFTTT остановились из-за сбоя в работе инфраструктуры Amazon, и пока они не ожили, пользователи потеряли контроль над своими «умными домами».

Срок годности вашего «умного дома» подошел к концу

Проблемы могут быть связаны не только с перебоями в работе ЦОД. Когда-то давно (до 2014 года, если быть точным) существовала небольшая компания Revolv, которая производила смарт-хабы. Это умные коробочки, которые служат центром «умных домов» и позволяют управлять компонентами их системы через мобильное приложение. Хабы и приложение общались друг с другом через сервер.

Как вы знаете, компании продаются и покупаются, что и произошло с Revolv — ее приобрел более крупный поставщик решений для «умного дома», компания Nest. Которую, в свою очередь, за несколько месяцев до сделки поглотила компания Google.

Сразу после приобретения конкурента Nest прекратила продажи смарт-хабов Revolv. Уже проданные устройства некоторое время продолжали работать, но в 2016 году в Nest решили полностью избавиться от наследия Revolv и отключили серверы, на которых держалась инфраструктура поглощенной компании.

Таким образом, в мае 2016 года смарт-хабы Revolv стали абсолютно бесполезными. Они просто-напросто ничего больше не делали. Ничегошеньки. Приложение тоже перестало работать. В 2014 году хабы Revolv продавались по $300 за штуку — отличная цена за устройство, которое через пару лет превратится в никчемную пластиковую коробку.

Ваша лампочка несовместима с GDPR

Когда вступил в силу Общий регламент по защите данных ЕС (он же GDPR — документ, определяющий порядок обработки данных), в Интернете многое изменилось. Помимо всего прочего, некоторые американские сайты перестали открываться с европейских IP-адресов, поскольку их владельцы, опасаясь штрафов за неправильную обработку данных европейцев, решили просто с ними не связываться.

Регламент GDPR повлиял и на вполне реальные объекты, ведь сейчас виртуальная среда очень тесно связана с физической. Например, в Европе «умные» лампочки Xiaomi Yeelight с управлением через приложение полностью утратили свои умные функции после GDPR-совместимого обновления. Они превратились в обычные лампочки, которые загораются только по нажатию выключателя. Конечно, это лучше, чем полная неработоспособность, но, скорее всего, у покупателей были несколько другие ожидания.

Робот-пылесос шпион

Все злоключения, о которых мы написали выше, никак не связаны с действиями пользователей: термостаты Netatmo, хабы Revolv и лампочки Yeelight работали бы отлично и дальше, если бы не происходило всякое на стороне серверов. А что на этих серверах происходит на самом деле — это вообще отдельная история.

Разработчики гаджетов для «умных домов» собирают и обрабатывают данные, которые получают от своих приложений и устройств. Им это нужно, во-первых, для того, чтобы поддерживать функциональность «умных» устройств, а во-вторых, чтобы разрабатывать новые возможности. Ну и, конечно, чтобы получше вас узнать. Ах да, еще некоторые разработчики приторговывают собранной информацией.

То, что наши данные стали разменной монетой корпораций, ни для кого не новость (если, конечно, вы не провели последний десяток лет в глуши тайги). Но не все хорошо понимают, какую информацию о нас собирают поставщики «умных» устройств и как именно они это делают. То есть мы, например, знаем, что Google и Facebook что-то там собирают, когда мы ходим по Интернету или сидим в соцсетях. Но понимают ли все пользователи Nest, что сама Nest уже в кармане Google, и что теперь Google владеет, к примеру, информацией о том, какая температура установлена в их доме?

А в курсе ли владельцы роботов-пылесосов iRobot, что iRobot и Google недавно заключили соглашение, где, в числе прочего, говорится, что Google сможет заглянуть в карты помещений, составленные роботами-пылесосами? По сути, компания пополнила и без того огромную копилку ваших личных данных планировкой дома.

Не только Google и Facebook одержимы данными о своих пользователях — компания Xiaomi тоже фиксирует планы помещений с помощью своих роботов-пылесосов Xiaomi Mi Robot и автоматически загружает их себе на сервер. Любопытный факт: роботы-пылесосы Xiaomi управляются через приложение, которое работает только при подключении к серверу (и для большинства пользователей это сервер, который находится в Китае).

Завершающий удар

Перевешивают ли все эти проблемы удобство удаленного управления бытовыми приборами — каждый решает сам. Но мы перечислили далеко не все неприятности — было еще несколько серьезных инцидентов с «умными домами». В октябре этого года что-то случилось с приложением, управляющим «умной» охранной сигнализацией Yale, — это привело к чудовищной неразберихе в домах с этой системой. Людям пришлось оставаться дома, потому что они не могли выключить воющую сирену. Инженеры Yale устраняли эту проблему более суток.

Ранее схожие неполадки возникли с «умными» замками производства Lockstate: при очередном обновлении прошивки возникли проблемы, и все «умные» замки полностью вышли из строя — превратились в «кирпичи».

Кто вообще пользуется «умными» замками? Оказывается, они очень популярны среди тех, кто сдает квартиры и дома через AirBNB. От сбоя пострадало более 200 гостей, которые просто не смогли войти в арендованные квартиры. Самое неприятное, что проблему невозможно было оперативно устранить, разослав обновленную прошивку удаленно — владельцам пришлось демонтировать замки и отправлять их производителю на ремонт или дожидаться, когда до них доберется инженер и заменит их. И в том, и в другом случае ждать приходилось по 2–3 недели.

Мы называем устройства, подключенные к сети, интернетом вещей. Но на самом деле стоило бы называть их вещами Интернета. Ведь они полностью зависят от сети, и если происходит какой-то сбой — отказ сервера, баги в приложении или прошивке, проблемы с подключением или какие-то другие напасти, — они моментально сходят с ума. В лучшем случае, гаджеты становятся лишь частично работоспособными, ну, а в худшем — превращаются в полностью бесполезные «кирпичи».

Источник: ***www.kaspersky.ru/blog/things-of-internet/21818/***