Надежная крепость

Умный дом без облачных технологий — возможно ли это? Мы проверим, насколько хорошо работают системы производителей без Интернета, и дадим советы о том, как сделать свой дом безопасным.

В Европе умные дома сейчас в тренде: еще никогда не был так высок спрос на умные системы безопасности, управляемые осветительные устройства и кондиционеры, а также на домашнюю автоматику, позволяющую производить ее дооснащение. Согласно данным статистического портала Statista, в этом году только в Германии жители потратят на системы SmartHome около 1,3 млрд евро. И таким образом они будут находиться на третьем месте в мире — сразу после США и Китая.

Причины подобного бума многообразны: если раньше автоматизация жилища была связана с большими затратами, то теперь все большее число производителей выходит на рынок с недорогими частными решениями. Многие люди по своей природе имеют потребность в безопасности, будь то защита от грабителей, от пожара или прорыва трубы. Теперь им предлагаются соответствующие продукты, которые дают возможность контроля над своим домом. Невозможно переоценить и фактор комфорта, когда есть управляемое освещение и отопление. В некотором роде способствует такой популярности и государство: с одной стороны, одним из требований кредитных учреждений для новостроек в Германии стало, например, дооснащение защитой от взлома, с другой стороны, принимаются новые законы, по которым обязательной становится установка детекторов дыма.

Обязательность облака и сервера — уязвимость системы

Как бы высоко люди ни оценивали системы для умного дома, одновременно присутствует и изрядная доля скепсиса по отношению к продуктам — просто потому, что зачастую их невозможно использовать без доступа в Интернет и облачных сервисов. И эти опасения нельзя назвать необоснованными, ведь подтверждений уязвимости умных домов достаточно. Поставщик услуг безопасности Sophos в настоящее время проводит эксперимент с системой умного дома, которая представляет собой заманчивую цель для хакеров. Процесс строительства, который можно было увидеть в прямой трансляции на CeBIT, очень выразительно демонстрирует, что умный дом точно так же сканируется злоумышленниками на наличие уязвимых мест, как домашний компьютер или сервер. А количество незащищенных систем бесчисленно: в прошлом году

ФОТО: Nest; Mumbi; Panasonic

дискаунтер Aldi продавал IP-веб-камеру, которую можно было использовать без установки пароля. Следствием такой опрометчивости становится незащищенная потоковая трансляция в режиме реального времени прямо из собственной гостиной. Хотя продавец и предоставляет обновление, его нужно устанавливать в ручном режиме. И модель веб-камеры Aldi — это далеко не единственный случай, который выдает простой поиск Google на запрос «незащищенные камеры».

В поисках безопасного продукта пользователи натыкаются на целые полчища производителей, использующих десятки собственных стандартов сигнализации и стандартов безопасности, которые никто не может по-настоящему проверить. Сюда же добавляется слабая инструкция по применению и ручной режим обновления микропрограммного обеспечения, создающий проблемы для пользователей, которые недостаточно разбираются в технике. В начале марта группа хакеров Exploitee.rs продемонстрировала две основные уязвимости популярного сетевого накопителя My Cloud от Western Digital: каждому из хакеров удалось стать администратором NAS, просто изменив сеансовые файлы cookie. А вторая ошибка позволила получить доступ через простую манипуляцию с PHP — на данный момент производитель закрыл только уязвимости, связанные с файлами cookie.

Эффективно защитить умный дом можно разными способами, о которых мы вам и расскажем. Разумеется, наилучшая защита — это независимая система, которая может функционировать и без доступа в Интернет. Но остается вопрос: кто такую предложит?

Полная функциональность без облака — редкость

Мы расспросили самых крупных производителей систем оборудования для умного дома, какова функциональность их систем без Интернета и какие лишения при этом придется терпеть. Например, системы освещения Philips Hue и Osram Lightify можно использовать без доступа в Интернет — впрочем, ничего другого от управления лампами и не ожидалось. Правда, при настройке программы для работы светильников системы Osram Интернет все-таки потребуется. Для управления системой через приложение для смартфона, само собой, также нужен доступ к Сети. То же самое действует для Home Base от Qivicon в отношении их облачных сервисов, например, при управлении веб-камерой. В остальном управление и настройка устройств Qivicon производится через WLAN — умные функции встроены в базовую станцию. Абсолютно похоже все выглядит у продуктов для умного дома от Devolo.

Такой производитель, как Innogy, делает попытки по предоставлению пользователям максимум независимости. После выполнения настроек умного дома базовая станция в остальное время может обходиться без подключения к Интернету. Помимо систем безопасности и кондиционирования, Innogy предоставляет и умные рольставни, практически полностью обеспечивая пользователя оборудованием для умного дома. Оборудование компании HomeMatic, предлагающей, пожалуй, самый широкий ассортимент для автоматизации дома, также может работать автономно без доступа в Интернет. То же касается систем Eqiva, которые, как и HomeMatic, вышли из eQ-3. В случае с HomeMatic IP, представляющим собой чистое облачное решение, что следует из названия, без Сети обойтись невозможно.

Абсолютно новой на европейском рынке является компания Nest, бывшее подразделение Google, со своими детекторами дыма, а также с внутренними и наружными камерами. →

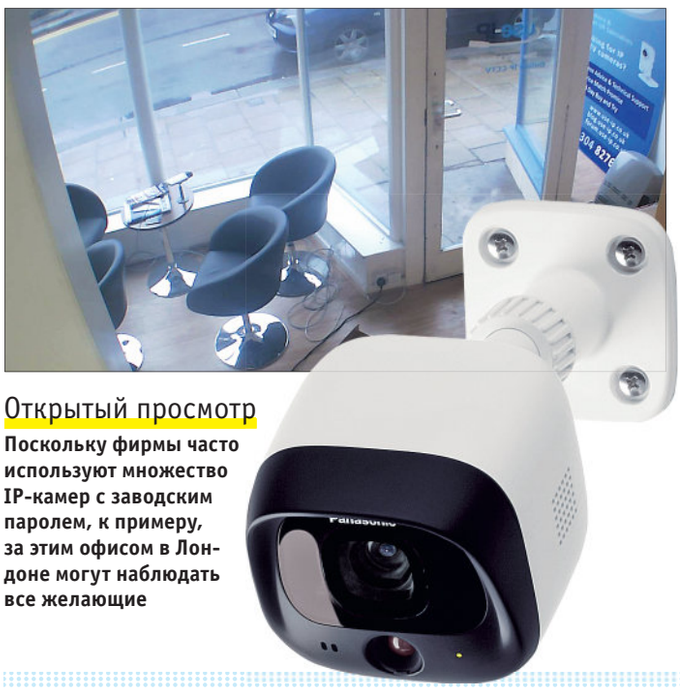
Оснащение детекторами дыма

С введением нормы об обязательной установке детекторов дыма в ряде европейских стран устанавливают все больше умных приборов пожарной сигнализации, которые включаются в Сеть или отправляют сигнал тревоги через облачный сервис прямо на смартфон.

> Новые детекторы дыма должны соответствовать требованиям DIN 14604. В них входит, к примеру, уровень сигнала не ниже 85 дБ(А), тестовая функция и раннее предупреждение о замене батареи.

> Ценовой диапазон составляет от нескольких сот рублей за простые устройства до 10 000 — 15 000 рублей за модели со смарт-функциями и облачной поддержкой. Если кто-то опасается за доступ к облаку, можно использовать детекторы дыма с радиосигналом, которые соединяются через сеть только друг с другом. Если случится возгорание в подвале, сработает и детектор в спальне. Радиодетекторы в большинстве случаев продаются в комплекте и стоят от 1500 рублей за штуку.

Детекторы дыма с радиосигналом Mumbi (около 6000 рублей за шесть штук) объединяются в сеть друг с другом и соответствуют стандарту систем пожарной безопасности DIN 14604



Открытый просмотр

Поскольку фирмы часто используют множество IP-камер с заводским паролем, к примеру, за этим офисом в Лондоне могут наблюдать все желающие

Центр управления в облаке

Пока устройства не соединены в умную сеть между собой, система для умного дома Medion обходится без облака

Широкая функциональность

Компания Nest предлагает продукты премиум-класса: 1 Nest Protect помимо дыма определяет и угарный газ. 2 Внутренняя камера имеет универсальное управление

Nest

Продукты для умного дома от компании, которая прежде была подразделением Google, теперь доступны и в Европе — во всяком случае, детектор дыма Protect с внутренней и наружной камерами. Термостат Nest появится в продаже в ближайшее время.

> Устройства премиум-класса от Nest можно использовать и без привязки к облаку, если не планируется установка удаленного доступа.

> Детектор дыма распознает угарный газ. При выделении дыма он сначала дает жильцам речевое предупреждение, а уже потом срабатывает сирена. Цены — около 8000 рублей за датчик и 14 000 рублей за камеры.

Если отказаться от удаленного доступа, то детекторы дыма и термостат работают и без подключения к Интернету. Однако обновления и здесь устанавливаются только через облако. А обеим камерам Nest доступ к облачному сервису требуется постоянно. С недавних пор и компания Medion вошла в число поставщиков решений для умного дома и предлагает достаточно широкие варианты с датчиками движения и детекторами дыма, IP-камерой, включаемыми розетками и светодиодными лампами. Здесь центр управления также встроен в базовую станцию и в принципе обходится без Сети. Правда, если друг с другом соединяются два действующих элемента, например, датчик движения и камера, то без облачного сервиса все же не обойтись.

Облачные сервисы как аргумент экономической целесообразности

У D-Link без доступа к Интернету вообще ничего не работает: любое взаимодействие между приложением для управления и системой проходит через облачный сервис mydlink. Правда, таймер и веб-камеры с уже установленными настройками дальше могут работать без Интернета. Для защиты от взлома D-Link даже дает рекомендацию по использованию маршрутизатора с резервным каналом UMTS, чтобы могли продолжать функционировать системы сигнализации после того, как DSL или кабельное соединение станут недоступны.

В системах для умного дома Mobilcom-Debitel нет единообразия. В частности, управление отоплением работает без Интернета, а в отношении безопасности и контроля облачный сервис вообще становится поводом для приобретения. Так, камера Smartfrog соединяется исключительно с облаком и сохраняет видеоконтент только на серверах Mobilcom. Поставщик обосновывает это более высоким уровнем безопасности, ведь при взломах грабители часто забирают с собой камеры с SD-картами, особенно в тех случаях, когда камеры расположены так, что любой посторонний человек может легко обнаружить их и извлечь.

Системы контроля Mobilcom-Debitel имеют собственные охранные функции, которые срабатывают, если бьют тревогу датчики движения или оконные датчики — понятно, что здесь не обойтись без прямой связи с облаком. Кроме того, облачный сервис Mobilcom в отличие от других сервисов реагирует на отключение кабеля DSL — например, при проникновении в жилище. Поэтому базовая станция включает в себя бэкап-маршрутизатор с UMTS, который в этом случае все равно передаст сигнал тревоги. Система бесперебойного энергоснабжения, которой оснащена базовая станция, при отключении электричества позволяет функциям безопасности действовать еще около 48 часов. К тому же Mobilcom-Debitel — единственная компания, предлагающая системы только в аренду.

Защитить умный дом самостоятельно

Итак, большинство систем для умного дома можно использовать и без доступа в Интернет — тем или иным образом. При использовании удаленного доступа и — прежде всего — при обновлении микропрограммного обеспечения без облачных сервисов, разумеется, не обойтись. Тем не менее можно принять меры, которые позволят снизить риск нападения на умные дома. Так, для всех устройств, которые требуют доступа в Интернет, следует использовать только надежные пароли. Более того, нужно изменить имя стандартного аккаунта «Admin» или деактивировать его. Многие хакеры сканируют Сеть в по-

ФОТО: компании-производители

исках таких стандартных пользователей, и это в особенности касается IP-веб-камер. Микропрограммное обеспечение также всегда должно быть актуальным, и здесь лучше не полагаться на то, что оно будет установлено автоматически. К тому же IP-камеры почти всегда автоматически регистрируются на веб-сервере в начале их эксплуатации — это удобно, поскольку потоковая передача в режиме реального времени идет напрямую через сайт независимо от места и от устройства. С другой стороны, такая регистрация — это широко открытая дверь для хакеров. Возможно, будет целесообразно полностью закрыть доступ в Интернет для слишком интересных с точки зрения хакеров устройств. Это можно настроить через веб-интерфейс роутера: у актуальных моделей ASUS это делается в меню «Дополнительные настройки/WAN» в разделе «Перенаправление портов» (или «Port Forwarding»).

Гостевая сеть и VPN надежнее

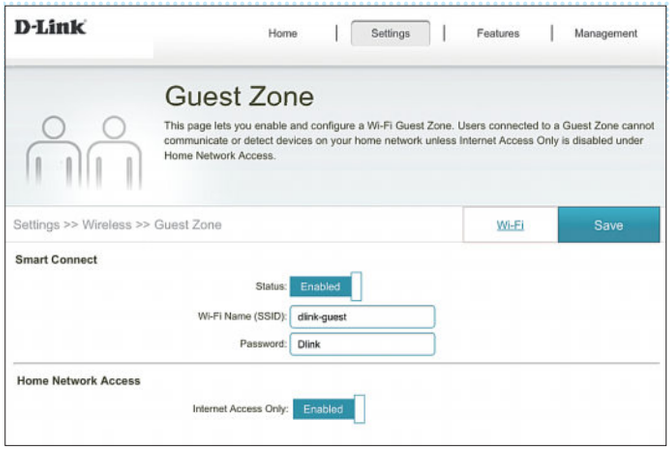
Последующая стратегия для повышения уровня безопасности: все устройства в системе умного дома должны быть подключены к собственной сети WLAN. Для этого необязательно требуется второй роутер, так как многие актуальные модели позволяют создавать гостевые сети. Они обеспечивают доступ в Интернет, но не к данным и устройствам в основной WLAN. Такое разделение также означает, что после настройки достаточно будет одного клика, чтобы отключить от Интернета систему умного дома. При изменении конфигураций или обновлении микропрограммного обеспечения можно будет с легкостью снова активировать доступ в Сеть.

При использовании виртуальной частной сети Virtual Private Network (VPN) можно получать закодированный доступ к компонентам умного дома без обходного пути через облачный сервер. С Raspberry Pi и OpenVPN можно также создать свой VPN-сервер. Таким образом, и вне дома мобильный телефон, с которого осуществляется контроль и управление системой умного дома, останется частью домашней сети LAN.

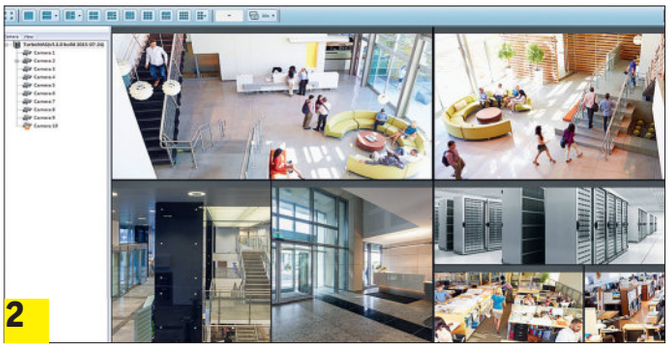
NAS как сервер видеонаблюдения

Если требуется запись и хранение видеоматериала с сетевых IP-камер, необходим постоянно работающий компьютер с большим объемом памяти — идеальная задача для сетевого хранилища (NAS). Такие производители, как Synology и QNAP, для многих из своих NAS предоставляют соответствующее приложение. С его помощью локальные IP-камеры соединяются с NAS. У QNAP для этого загружается Surveillance Station из центра приложений операционной системы NAS. Сначала нужно запустить IP-камеры с роутером через локальный ПК. Затем необходимо настроить запись и вывод видеопотока в приложении Surveillance Station. Картинка с камер будет отображаться либо в приложении для ПК, либо в веб-интерфейсе Surveillance Station. При этом можно выводить изображение с нескольких камер одновременно, а также будет возможным управление поворотными камерами. С помощью дополнительного приложения (QUSBCam) для контроля за домом можно использовать даже USB-веб-камеры. В случае с моделями для NAS марки Synology видеостанция работает аналогичным образом. NAS следует оборудовать так, чтобы она оставалась незаметной и недоступной для взломщиков.

Если соблюдать стандарты безопасности, всегда использовать актуальное микропрограммное обеспечение, правильно обезопасить роутер и WLAN, а также по возможности задействовать VPN-соединение, то можно со спокойной совестью вливаться в популярный тренд и делать свой дом умным.



С помощью гостевой сети можно отделить устройства системы умного дома от компьютеров в домашней сети WLAN



Видеостанция

Приложения для организации сервера видеонаблюдения на базе NAS от 1 Synology и 2 QNAP позволяют использовать IP-камеры локально и предлагают пользователям множество функций

HomeMatic IP

Представляет собой чистое облачное решение от eQ-3 и соединяется даже с помощником Amazon Alexa для голосового управления компонентами