информационные технологии

Зомби-апокалипсис

На Mobile World Congress-2017 в конце февраля в Барселоне «Лаборатория Касперского» при участии футуролога Яна Пирсона нарисовала счастливое цифровое будущее человечества. Правда, с оговоркой: все будет хорошо, если мы научимся противостоять новым угрозам, которые несет повсеместная цифровизация. Мы уже справились с BYOD и мобильностью. Следующую волну проблем для безопасников несет интернет вещей.

ЕВГЕНИЙ ПАВЛЕНКО

— сегмент рынка —

Интернет вещей, как потребительский, так и промышленный, уже пришел в нашу жизнь. Даже скорее ворвался через все эти китайские noname-чайники с Wi-Fi, не очень «умные», но подключенные к интернету розетки, браслеты, видеокамеры, весы и все что угодно.

Аналитики IDC сообщают, что в России эти технологии активно осваивают три отрасли: производство, транспорт и энергетика. На них приходится половина от общего объема рынка IoT. На четвертом месте идет госсектор, который в основном вкладывается в развитие «умных» городов.

Самый многообещающий и быстрорастущий сегмент в РФ на рынке IoT — страхование, где уровень инвестиций, по мнению IDC, будет увеличиваться в два раза быстрее, чем на других направлениях. Также будут набирать объем кросс-отраслевые решения, которые могут использоваться в разных сферах по похожим сценариям.

По подсчетам AC&M Consulting, в стране на конец прошлого года уже функционировало 10 млн IoT-устройств. В сфере ЖКХ, по данным iKS-Consulting, в России в 2016 году работал 1,1 млн подключенных объектов, а через три года их будет уже 5,2 млн. Решения для IoT разрабатывают телеком-компании вместе с вендорами. В марте «МегаФон» с Huaewei объявили о выпуске решения для этой сферы на основе стандарта NB-IoT, который позволяет подключенным устройствам работать до десяти лет без замены. МТС уже предлагает специальный тариф для IoT «Умное устройство» с оплатой сразу за год. Этот оператор лидирует на рынке интернета вещей с долей 40%, по данным AC&M Consulting. На втором месте идет «МегаФон» (35%), за ним следует «Вымпелком (19%).

Безответственность производителей

В целом понятно, зачем эти подключенные устройства могут понадобиться потребителям. Также очевидно, что это источник доходов для операторов. Для бизнеса IoT и его промышленная модификация IIoT нужны по двум причинам: чтобы собирать данные, которые могут оказать важнейшее влияние на деятельность компании, а также чтобы противостоять различным видам мошенничества.

Но первое порождает новые угрозы, что, возможно, нивелирует пользу второго. Согласно прогнозам Gartner, в будущем бизнес станет все больше склоняться к датацентричной модели информационной безопасности. Как говорят аналитики этой компании, экспоненциальный рост объемов данных, сбор их из множества разных источников, обработка и хранение требуют пересмотра существующих моделей защиты данных и архитектуры систем информационной безопасности. По их мнению, к 2020 году 40% инструментов, которыми пользуются крупные предприятия для информационной защиты данных, окажутся заменены средствами дата-центричного аудита и защиты. Сейчас их доля меньше 5%. Специфика этих решений состоит в том, что они позволяют централизованно управлять пользователями и администраторами и наблюдать, как они используют те или иные наборы данных.

Но это далеко не все, что требуется изменить в подходах и инструментах ИБ в связи с распространением IoT/IIoT. Прошлый год в сфере информационной безопасности стал годом Mirai — ботнета, собранного из нескольких сотен тысяч взломанных подключенных устройств. Простенькая программа с помощью перебора шести десятков стандартных паролей пачками превращала веб-камеры, роутеры и другие устройства в IoT-зомби. Mirai устроила самую крупную DDoS-атаку в истории интернета: на жертву обрушивался терабит мусорных данных каждую секунду.

Откуда взялись устройства в этом ботнете? Ну, например, команда безопасности Android недавно отчиталась о том, что «всего» 0,05% устройств с этой системой содержали в прошлом году потенциально опасные приложения (приложения с бэкдорами, трояны и прочие). Это значит, что 700 тыс. девайсов из 1,4 млрд существующих в мире, заведомо находятся под угрозой. Если учесть, что обновления системы защиты установили в прошлом году лишь на 735 млн устройств с этой ОС, ситуация выглядит совсем удручающе.

А ведь так обстоят дела с активно используемыми устройствами. Страшно представить, сколько паразитных программ может внедриться в IoT-объекты, к которым годами никто не подходит, например счетчики воды или термостаты. Одна из главных угроз со стороны интернета вещей, по словам Дмитрия Огородникова, директора центра компетенций по информационной безопасности компании «Техносерв»,— именно DDoS-атаки и общий объем паразитного трафика.

Андрей Никишин, руководитель отдела развития технологических проектов «Лаборатории Касперского», добавляет: «Мы полагаем, что Mirai — это вершина айсберга атак и заражений подобных устройств. К сожалению, разработчики IoT-устройств не уделяют должного внимания вопросам кибербезопасности. Подобные устройства крайне редко обновляются и остаются уязвимыми месяцы и годы».

Александр Лямин, глава Qrator Labs, рисует печальную картину: «Интернет вещей не готов для инфраструктуры интернета. Можно сравнить интернет с автомагистралью highway. Что будет, если на эту скоростную трассу выпустят автомобиль, не отвечающий стандартам безопасности? Более того, у этого автомобиля порой не работают тормоза и производитель не заботится о его техподдержке. Это небезопасно как для водителя, так и для всех окружающих. Интернет вещей — это целая армада подобных автомобилей, заполонивших более или менее работающий интернет. Никто не рассчитывал на движение таких некачественных „развалюх“».

Алексей Качалин, заместитель директора по развитию бизнеса в России компании Positive Technologies, добавляет, что для злоумышленников могут также представлять интерес устройства, которые можно заблокировать. Уже случались инциденты с «локерами» «умных» кондиционеров и телевизоров. Большой интерес у злоумышленников вызывают и автономные дроны. Манипулируя ими, можно получить данные, перехватить управление, похитить дорогостоящее устройства, а иногда (в случае с военными дронами) — получить доступ к боевому вооружению.

Маршрут построен

По мнению ряда экспертов, инфраструктура интернета в той или иной степени готова принять трафик IoT/IIoT. Андрей Никишин говорит: «Я не вижу больших проблем с точки зрения пропускной способности каналов. Сейчас продвигается парадигма, при которой большая часть вычислений будет проводиться или на уровне самих „вещей“ или на уровне локальных хабов и в облако будут передаваться проценты от информации, которая генерируется подключенными вещами. Также многие компании разворачивают приватные облака для работы с IoT-устройствами».

Но и здесь не все так хорошо. Андрей Янкин, руководитель отдела консалтинга Центра информационной безопасности компании «Инфосистемы Джет», предупреждает: «Рост объемов подключенных к интернету устройств вновь поднимает вопрос о необходимости перехода с адресации IPv4 на IPv6. Хотя протокол IPv6 по архитектуре намного безопаснее IPv4, уверен, в бурное время перехода на новые технологии возникнет огромное число специфических угроз ИБ».

Дмитрий Огородников напоминает о том, что существует и другая проблема — отсутствие общих стандартов, протоколов, архитектур этих инфраструктур и их взаимодействия. «Основные принципы построения интернета вещей только начинают разрабатываться, многое находится на уровне определений и рекомендаций — вы должны об этом подумать сами. Вместе с тем подключение сенсоров и особенно исполнительных механизмов (Actuator) несет в себе новые риски некорректного управления объектами технологических процессов или жизнеобеспечения. Большинство известных атак на объекты АСУ ТП были направлены на контроллеры PLC и изменение режима работы этих устройств. Эти контроллеры не подключаются напрямую к интернету, поэтому атакующие были вынуждены воздействовать на управляющие системы для последующего контроля конечных устройств PLC. Но интернет вещей создается по принципу „все, что может подключаться, должно быть подключено“. При такой концепции и без единых стандартов риски возрастают многократно».

с15

«ИНТЕГРИРОВАННАЯ И ЗАЩИЩЕННАЯ ПЛАТФОРМА НА СЕГОДНЯШНИЙ ДЕНЬ ОТСУТСТВУЕТ»

Руководитель сектора ИБ компании AT Consulting АНТОН КАРДАНОВ видит в интернете вещей источник проблем для отделов компаний, следящих за информационной безопасностью.

ПРЕДОСТАВЛЕНО AT CONSULTING

— Видите ли вы рост угроз, связанных с распространением интернета вещей, подключением критичной инфраструктуры к интернету и т. д.?

— Подключение критичной инфраструктуры к сети с неограниченным числом пользователей с практически неограниченными возможностями крайне опасно. Необходимо либо отказываться от такого подключения, либо в случае обоснованной необходимости применять максимально надежные меры защиты.

Появление интернета вещей, как и любой другой новой технологии, порождает и новые угрозы, а с учетом того, что интернет вещей — это объединение набора технологий под единым брендом, то и угрозы у него общие, объединенные в «одном месте».

— Какие новые типы угроз возникли за последние два-три года, чем они страшны бизнесу?

— Для того чтобы понять, какие угрозы появились за последнее время, нужно посмотреть, что новое появилось в мире ИТ, какие технологии наиболее востребованы. Редкий «среднестатистический» злоумышленник будет серьезно прорабатывать эксплуатацию уязвимости редко встречающейся технологии. Гораздо интереснее масштабность.

В последнее время все большую популярность набирают облачные ресурсы, значительно вырос парк мобильных устройств, что способствовало вектору развития угроз в данном направлении. Стали актуальны таргетированные атаки, направленные на конкретные инфраструктурные сегменты и использующие актуальные для этих сегментов уязвимости.

Для различного бизнеса важны различные характеристики безопасности: для кого-то важно соблюдение конфиденциальности, для кого-то — доступности; комплексный подход при атаках на бизнес может привести к отказам по «всем направлениям», поэтому и система защиты должна быть комплексной.

— Какова готовность инфраструктуры интернета, всеобщей ИТ-экосистемы, в которой «живут» и функционируют компании из разных сфер, к приходу интернета вещей и промышленного интернета вещей? Способны ли сети справиться с новыми (даже легитимными) нагрузками и с новыми угрозами?

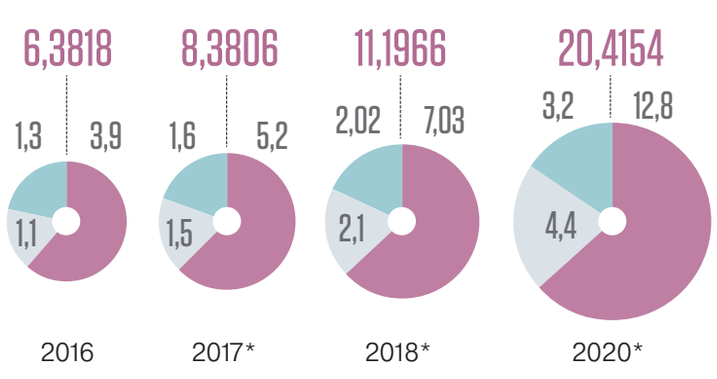
— Что касается текущих сетей, то их готовность противостоять вновь появляющимся киберугрозам различна: кто-то во главе подхода ставит бизнес без учета интересов информационной безопасности, кто-то старается реализовать базовые, кто-то — продвинутые меры защиты. Единая же интегрированная и защищенная платформа на сегодняшний день отсутствует.

— Какие варианты решения этих проблем вы можете предложить? Можно ли бороться с новыми угрозами старыми методами? Какие новые подходы, продукты или даже классы продуктов и услуг, регуляторные инициативы (что-то еще) могут стать ответом на растущие риски, связанные с киберугрозами?

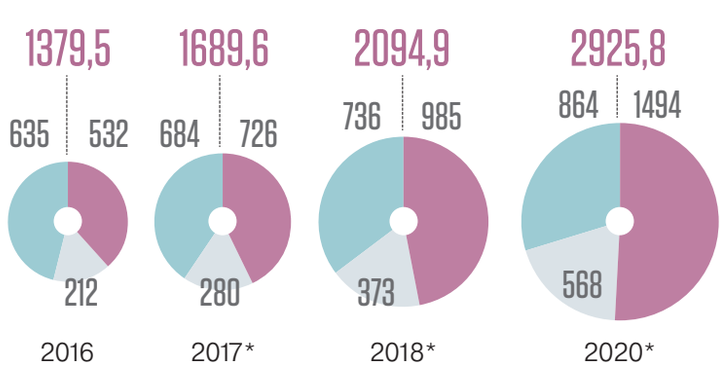
— В настоящее время прорабатываются подходы к построению единой защищенной инфраструктуры для умных домов и интернета вещей. Такая инфраструктура будет предоставляться как услуга и позволит минимизировать риски, возникающие совместно с интеллектуализацией бытовых условий современного мира.

БЛЕСК И ОПАСНОСТЬ ИНТЕРНЕТА ВЕЩЕЙ

ЧИСЛО IOT-УСТРОЙСТВ В МИРЕ (МЛРД ШТ.)



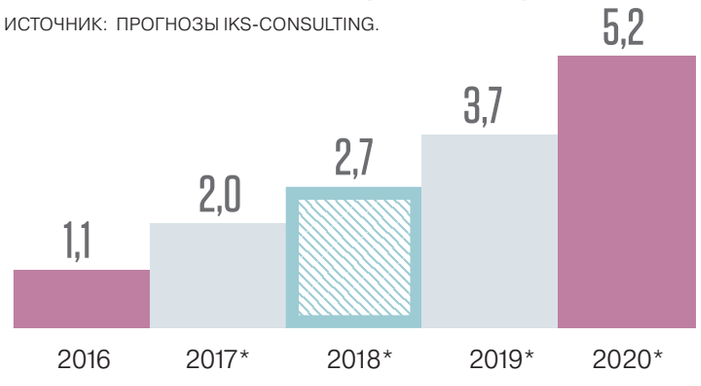
ЗАТРАТЫ КОНЕЧНЫХ ПОТРЕБИТЕЛЕЙ НА IOT ($ МЛН)



ПОТРЕБИТЕЛЬСКИЙ РЫНОК | БИЗНЕС: КРОСС-ИНДУСТРИАЛЬНЫЕ РЕШЕНИЯ | БИЗНЕС: СПЕЦИФИЧЕСКИЕ УСТРОЙСТВА ПО ВЕРТИКАЛЯМ

КОЛИЧЕСТВО ПОДКЛЮЧЕННЫХ ОБЪЕКТОВ ЖКХ В РФ (МЛН ШТ.)

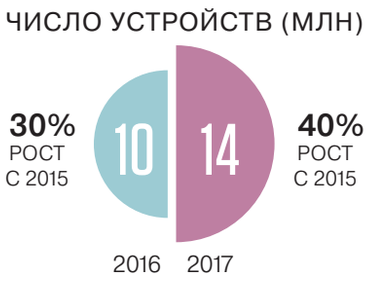
ИСТОЧНИК: ПРОГНОЗЫ IKS-CONSULTING.



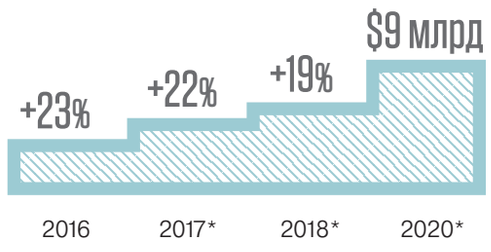
*ПРОГНОЗ.

IOT В РОССИИ

ЧИСЛО УСТРОЙСТВ (МЛН)



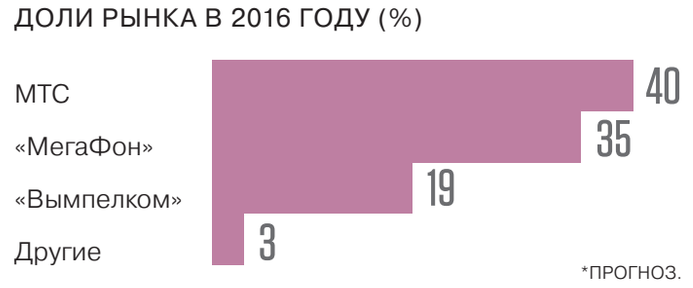
ОБЪЕМ РЫНКА



ИНВЕСТИЦИИ В **IOT/IIOT**

$4 млрд инвестированы в оборудование, программное обеспечение, услуги и связь в 2016 году

ДОЛИ РЫНКА В 2016 ГОДУ (%)



*ПРОГНОЗ.

РИСКИ

MIRAI — ПЕРВЫЙ В МИРЕ **IOT-БОТНЕТ** И КРУПНЕЙШИЙ ЗА ВСЮ ИСТОРИЮ

500 целей были атакованы в 2016 году

1,2 Тб/сек. максимальная скорость атак

145 тыс. взломанных IoT-устройств в ботнете

ИСТОЧНИКИ: GARTNER, TRIPWIRE, KASPERSKY LAB, IKS-CONSULTING, AC&M CONSULTING.

ОПАСЕНИЯ ПРОФЕССИОНАЛОВ ИБ В 2017 ГОДУ

96% ожидают атак на критическую инфраструктуру промышленного интернета вещей (IIoT) в энергетике, ЖКХ, госслужбах, медицинских учреждениях и финансах.

94% отмечают рост угроз ИБ, в связи с распространением интернета вещей

64% осознали необходимость использования защиты от IIoT-атака

51% не готовы к таким атакам