Москва, 20.06.2014

Как справиться с неизвестными угрозами в сфере ИТ-безопасности

После обнаружения уязвимости Heartbleed никто больше не сомневается, что со временем будут выявляться все новые бреши в системах безопасности. Однако мы не знаем точно, с чем именно столкнемся. К чему нам следует готовиться и какие действия предпринимать?

Министр обороны США Дональд Рамсфельд вряд ли предвидел появление Heartbleed, но, безусловно, хорошо понимал критические угрозы информационной безопасности, которые внезапно выплыли на свет божий. «Существуют известные известные, – изрек он однажды фразу, впоследствии ставшую знаменитой. – Это вещи, о которых мы знаем, что мы их знаем. Существуют известные неизвестные. Это вещи, о которых мы знаем, что мы их не знаем. Но еще существуют неизвестные неизвестные. Это вещи, о которых мы не знаем, что мы их не знаем».

Heartbleed можно было бы отнести к последней категории, однако мы с вами слишком хорошо информированы, чтобы делать столь поспешные выводы. Ошибка в коде, который в том или ином виде используют две трети веб-сайтов, позволяет злоумышленникам похищать идентификаторы и пароли пользователей непосредственно из памяти сервера, не оставляя при этом следов.

С момента появления уязвимости Heartbleed до ее обнаружения «белыми» хакерами прошло целых два года. Доподлинно не известно, как давно преступные группировки и спецслужбы узнали об этой ошибке, если, конечно, они вообще были в курсе. Но это далеко не первый случай обнаружения серьезной проблемы с безопасностью в интернете.

два типа брешей

Критические ошибки безопасности делятся на две основные категории: ошибки проектирования и ошибки развертывания. В 2008 году Дэн Камински (Dan Kaminsky), гуру в сфере безопасности, который в то время был директором, отвечавшим за тестирование систем на предмет взлома в компании IOActive, обнаружил критическую ошибку проектирования в DNS. Она позволяла подменять IP-адреса доменов верхнего уровня и любых других. Дэн сумел объединить усилия крупнейших мировых интернет-компаний, и, действуя без лишней огласки, они устранили эту проблему.

Вирус-червь Conficker эксплуатировал уязвимость, связанную с ошибкой развертывания, которая была обнаружена в том же году. Своим стремительным распространением эта вредоносная программа обязана критической бреши в Windows, посредством которой компьютеры заражали друг друга. Существовали и другие серьезные угрозы.

На все уязвимости и ошибки, включая Heartbleed, специалисты чаще всего реагировали постфактум: паническими исправлениями, запоздалым созданием обучающего веб-сайта, шквалом тревожных статей в прессе. Точно можно сказать лишь одно: все последующие проблемы безопасности будут уже «известными неизвестными» по Рамсфельду. Мы знаем, что они есть, но не имеем понятия, что они из себя представляют.

переосмысление открытого исходного кода

Вооруженные этим знанием члены совета директоров лично отвечают за потенциальные убытки от эксплуатации подобных уязвимостей злоумышленниками, считает Джим Кениг (Jim Koenig), директор компании Booz Allen Hamilton, который также занимается обеспечением кибер- безопасности и ответными мерами на угрозы в интернете.

«Совет директоров будет нести ответственность за мониторинг и анализ рисков кибербезопасности, – заявил Кениг. – В том числе за риски, связанные с использованием программ с открытым кодом».

Уязвимость, обнаруженная в популярной системе OpenSSL, заставляет переосмыслить саму концепцию открытого исходного кода. Над проектом с годовым бюджетом около миллиона долларов США работали четыре инженера-программиста.

«Возможно, вначале этого было достаточно, – прокомментировал Кениг. – Но, учитывая, что де-факто эта система стала стандартом для SSL, встает вопрос о ее поддержке со стороны государственных органов и бизнеса, поскольку риски и зависимость потребителей от этого решения чрезвычайно высоки».

Он уверен, что компании должны вкладывать свои личные средства в совершенствование и усиление безопасности используемых ими продуктов с открытым исходным кодом. Например, в виде платежа за анализ кода, взимаемого всякий раз при оформлении лицензии.

Такой подход поможет защитить ПО с открытым исходным кодом, однако далеко не все критические проблемы безопасности связаны с программными продуктами этого типа. Например, открытые проекты не имели отношения к уязвимостям в MS-CHAP v2.0, которые Каталин Косой (Catalin Cosoi), главный стратег безопасности BitDefender, считает одними из самых серьезных за последние несколько лет. Каталин Косой подчеркивает, что облачные вычисления и управляемые сервисы распространяются все шире и шире, поэтому новые «известные неизвестные» будут, по его мнению, связаны именно с этими двумя направлениями. Он видит и положительные, и отрицательные последствия этой тенденции: «С одной стороны, существует опасность централизованного принятия ошибочных решений. С другой, благодаря таким сервисам компании открывают для себя невиданные ранее возможности».

Есть и другие преимущества, как отмечает Уилл Дорманн (Will Dormann), эксперт по анализу уязвимостей из группы CERT Института программной инженерии Университета Карнеги-Меллон. Он считает, что, когда речь идет о мониторинге и установке исправлений, может помочь консолидация трафика крупными провайдерами.

предприятия, будьте готовы

В конечном итоге корпоративные пользователи должны быть готовы к встрече с «известными неизвестными». Пако Хоуп (Paco Hope), главный консультант компании Cigital, специализирующейся на ИТ-безопасности, перефразируя Нассима Николаса Талеба, автора теории «Черный лебедь[1]», советует компаниям быть «антихрупкими» в своем стремлении к безопасности.

[1] **«Чёрный лебедь»** — теория, рассматривающая труднопрогнозируемые и редкие события, которые имеют значительные последствия. Автором теории является Нассим Николас Талеб, который в своей

«Ни в коем случае нельзя считать, что сбои исключены, – считает он. – Вместо этого следует свести уязвимость к минимуму и смириться с тем, что возможны неудачи. Поэтому мы готовим планы восстановления и постоянно проводим тренировки в условиях, приближенных к боевым. Наши сотрудники действуют с полным пониманием ситуации, применяя отработанные приемы и методы».

Уязвимость Heartbleed в очередной раз показала, что окружающий мир полон как «известных», так и «неизвестных неизвестных». В условиях высокой неопределенности важно быть готовым к быстрой адаптации и рассматривать столкновение с проблемами как опыт, на котором нужно учиться.

Узнайте, как мы можем помочь вашей компании.

книге «Чёрный лебедь. Под знаком непредсказуемости» ввёл термин «события типа „чёрный лебедь“» (англ. *TBS, The Black Swan*).