ЕВРОПА 14.07.2021 | Екатерина Венкина

Мировой лидер в области кибербезопасности

Весь мир пытается противостоять атакам «русских хакеров». Похоже, Дания вырывается вперед.

«Не открывайте это письмо от “Макдоналдса”». На экране телефона белыми буквами на зеленом фоне написано: «Предупреждения». Под ним надпись: «Vi er kede», что по-датски означает: «Нам очень жаль» – и желтая буква M. Она максимально знакома и автоматически напоминает о жирных бургерах и картошке фри – постыдном удовольствии после тяжелого рабочего дня.

Это уведомление – предупреждение о мошенническом электронном письме, замаскированном под сообщение от «Макдоналдса». Его отправило датское приложение Mit digitale selvforsvar («Моя цифровая самозащита»). По словам руководителя проекта Уллы Мэллинг, приложение «уже загрузили 250 тыс. раз с момента запуска в апреле 2017 года, и в среднем у него 80 тыс. активных пользователей в месяц».

Приложение предоставляет информацию о цифровом мошенничестве, угрозах от вирусов и вредоносных программ, оперативных обновлениях от банков и правоохранительных органов. Оно также дает конкретные советы на случай возникновения проблем с безопасностью. Инициатива является результатом сотрудничества между Датским советом потребителей (Forbrugerrådet Tænk), некоммерческой организацией TrygFonden, финансовым сектором и Датским советом по предупреждению преступности (Det Kriminalpræventive råd).

Что еще важнее, это приложение – воплощение датского подхода к информационной безопасности и кибербезопасности, в которой различные учреждения практически идеально взаимодействуют, а в центре внимания – повседневная безопасность граждан и компаний.

Дания: Primus inter pares

До недавнего времени Дания с населением чуть больше 5,8 млн человек оставалась в сфере кибербезопасности незамеченной, в тени таких больших игроков, как США, Израиль и Великобритания. Но сейчас, похоже, у нее наконец достаточно опыта, чтобы оказаться в центре внимания.

В этом году Министерство иностранных дел объявило, что Дания заняла первое место среди самых кибербезопасных стран мира со средним общим баллом 3,56, согласно данным британской исследовательской фирмы Comparitech. Как Дания этого добилась? Было ли это связано с тем, что страна мобилизовала свои усилия по обеспечению информационной безопасности после серьезного нарушения безопасности в 2015-2016 годах, которое, как считал Копенгаген, было связано с «разведывательными службами или центральными элементами в российском правительстве»?

«Очень критическая ситуация»

В апреле 2017 года копенгагенская газета Berlingske опубликовала отдельные выводы из отчета Центра кибербезопасности Службы военной разведки Дании (CFCS). Выяснилось, что та же хакерская группа, которая стояла за кибератакой 2016 года на серверы Демократической партии США, получила доступ к «учетным записям электронной почты отдельных членов датской обороны». Несмотря на то что данные, к которым был получен доступ, назвали незасекреченными, их все равно можно было бы использовать, «чтобы с помощью шантажа завербовать сотрудников как агентов», – сообщила CFCS.

Бывший тогда министр обороны Дании Клаус Хьорт Фредериксен оценил это нарушение как «чрезвычайно критическую ситуацию». По данным нескольких спецслужб, за атакой, скорее всего, стояла группа APT28, также известная как Fancy Bear, которая связана с российской военной разведкой.

Прошло всего четыре года с тех пор, как стало известно об атаке, и Дания уже возглавила рейтинг Comparitech как «самая кибербезопасная» страна в мире. По словам Ребекки Муди, ведущей исследовательницы рейтинга, Дания входила в тройку лучших 10 раз из 15. Там не было ни одного пользователя, подвергшегося атаке мобильных троянов-вымогателей и мобильных троянов в банкинге. Она также показала очень хорошие результаты в таких показателях, как процент пользователей, подвергшихся атакам троянов-

вымогателей (0,02%) и атакам криптомайнеров (0,11%).

Хотя исследование, основанное на данных «Лаборатории Касперского» за третий квартал 2020 года, в значительной степени ориентируется на вредоносное ПО и не дает более глубокого понимания правовых и стратегических вопросов (в Глобальном индексе кибербезопасности – 2018, где эта информация есть, Дания занимает 12-е место в европейском регионе с оценкой 0,85), оно все же показывает, в чем датчане особенно хороши: в индивидуальной цифровой гигиене и безопасности финансовых услуг.

Последний пункт как минимум частично связан с повсеместным внедрением двухфакторной аутентификации. Она успешно препятствует определенным векторам атак, учитывая, что личные цифровые подписи используются в качестве логина для всех государственных онлайн-сервисов и в финансовой сфере. Еще один революционный фактор – качественные банковские приложения.

Тревожный звонок

В течение следующих нескольких лет Дания планирует инвестировать не менее 1,5 млрд датских крон (202 млн евро) в кибербезопасность и информационную безопасность. Согласно стратегии правительства на 2018-2021 годы, политика включает три аспекта: повышение технологической устойчивости, информирование граждан и усиление координации между различными субъектами. Сейчас Дания активно работает над определением своей критической инфраструктуры. Это поможет правительству принять руководящие принципы готовности к чрезвычайным ситуациям и стратегии предотвращения нарушений.

Итак, означают ли эти планы, что Дания сделала выводы после серьезных проблем с безопасностью в 2015-2016 годах? Редактор исследования Comparitech Пол Бишофф говорит, что это вполне возможно, а вот Ребекка Муди оценивает ситуацию более осторожно: «Может быть. Думаю, всякий раз, когда кто-то подвергается успешной кибератаке, они склонны повышать и операционную безопасность, и кибербезопасность».

Ларс Байлум Холмгаард Кристенсен, исполнительный директор Датского центра кибербезопасности, вспоминает, как компании воспринимали нарушения безопасности, когда информация о них впервые стала достоянием общественности. «Думаю, для многих компаний это стало тревожным звоночком. После этих атак осведомленность об угрозах возросла», – говорит он.

В CFCS создан круглосуточный оперативный центр, который помогает поддерживать национальную карту осведомленности о ситуации с кибербезопасностью. Также было намечено 25 конкретных инициатив по консолидации защиты от кибератак, преступников в сфере информационных технологий и внешних угроз.

Поскольку утечка данных стала серьезным прецедентом, нетрудно предположить, что реакция датских спецслужб на нее должна была быть гораздо более систематической и тщательной, чем простой подход «давайте все исправим».

Более того, пример Дании как одной из стран НАТО, безусловно, показал, насколько хрупким стал технический баланс в мире, где большие данные в сочетании с возможностями искусственного интеллекта дают новое понимание цифровых уязвимостей на фоне увеличения числа атак киберпреступников.

Неоднозначная позиция Москвы

Даже несмотря на то, что «русские хакеры» продолжают восприниматься западным цифровым миром как «бунтовщики», позиция Москвы в отношении таких групп остается неоднозначной. С одной стороны, Кремль категорически отрицает причастность официальных российских структур к подобным атакам. С другой – у властей есть некая гордость, подкрепленная официальной пропагандой, относительно того, на что якобы способны российские айтишники.

Тем не менее, по словам Александра Исавнина, российского интернет-эксперта и преподавателя Свободного университета Москвы, «мы не можем говорить об особой неприязни «русских хакеров» к Дании». Их метод работы скорее заключается в том, чтобы атаковать одну уязвимость за другой (часто в разных странах), чтобы последовательно сломать несколько систем безопасности. Наиболее широко используемая версия интернет-протокола – IPv4 (в отличие от его преемника следующего поколения IPv6) – позволяет сканировать почти весь Интернет на наличие уязвимостей в течение нескольких минут благодаря ограниченному количеству IP-адресов и текущим скоростям соединения.

Более того, он признает, что лица, стоящие за такими атаками, могут быть самыми разными, будь то научные военные подразделения, аутсорсеры через различные технологические платформы, операторы наемного вредоносного ПО, школьники или современные IT-

эквиваленты советских «шарашек», исследовательских лабораторий в системе лагерей ГУЛАГ. Их оперативная цель в большинстве случаев – если не выуживать секретную и труднодоступную информацию, то создавать хаос. Сейчас такие нападения возможны вследствие отсутствия всемирно согласованных процедур воздействия на киберсубъекты.

Что дальше? Кибердизайн!

При всех этих улучшениях не следует забывать один важный фактор, безусловно, способствующий тому, что Дания занимает первое место в мировом рейтинге Comparitech. В отличие от США, Дания в настоящее время не воспринимается как серьезная цель кибератак.

Хотя, как показывает оценка CFCS за июнь 2021 года, уровень угрозы в контексте кибершпионажа и киберпреступлений очень высок, но опасность серьезных кибератак на датские власти и частные компании остается на низком уровне. Это значит, что с точки зрения датских спецслужб очень маловероятно, что в Дании в ближайшем будущем произойдет что-то вроде кибератаки через программы-вымогатели на Колониальный трубопровод в США.

Пока ситуация остается таковой, Дания, несомненно, будет и далее заниматься кибербезопасностью, используя методы, которые остальным странам представляются достаточно инновационными. В рамках международной деятельности она будет продолжать продвижение кибердипломатии. В 2017 году был назначен первый в мире «технический дипломат» для представления интересов страны в Кремниевой долине. Сейчас эту должность занимает технологический посол Анн Мари Энгтофт Ларсен, а первым ее занимал Каспер Клюнге.

Еще одна многообещающая сфера – сочетание различных решений в сфере кибербезопасности с инновационным датским дизайном, при котором соответствующие решения предлагаются в рамках продукта еще на этапе его разработки. По мере развития дискурса относительно этого нового рыночного мышления национальное бизнес-сообщество Дании, похоже, все больше склонно рассматривать кибербезопасность как новую сферу роста.



Екатерина Венкина

Екатерина Венкина (Ekaterina Venkina) — редактор новостей Deutschen Welle в Бонне, пишущая о мировой политике, а также региональных вопросах в России и странах бывшего СССР. На протяжении своей карьеры она жила, училась и работала в шести разных странах: России, Швеции, США, Великобритании, Бельгии и Германии. Венкина является членом союза журналистов n-ost в Берлине.