

Пользователей защитят

Пользователи интернета страдают от себе же подобных: именно от других людей на нас валится спам, атаки и прочие неприятности. В рамках академической сети LATNET действует специальная рабочая группа, которая позволяет предотвращать такие инциденты и эффективно с ними бороться. Сегодня мы общаемся с её руководителем Байбой Кашкиной и главным специалистом Артуром Меденисом.

Алексей ТАРАСОВ

alexey.tarasov@times.lv

За рубежом команды CERT (Computer Emergency Response Team) — вполне обычное дело. Они существуют во многих организациях и занимаются тем, что обеспечивают безопасность своих пользователей, предупреждая и устраняя различные угрозы из интернета или, как их называют ещё, "инциденты нарушения безопасности". Кроме того, они ищут виновных и сотрудничают с правоохранительными органами. В Латвии пока существуют только две таких команды — одна из них — LATNET CERT — работает в рамках академической сети этого провайдера. Вторая — в рамках VITA (Valsts Informācijas Tīkla Aģentūra).

— **Итак, что же такое — инцидент нарушения безопасности?**

— (Артур) Это и спам, и сканирование портов, которым обычно промышляют дети, начитавшиеся разных книг и журналов, и различные фишинг-атаки. Но этим, конечно же, дело не ограничивается — нельзя забывать и о попытках незаконного получения какой-либо информации и многом другом.

(Байба) Если давать общее определение, то можно сказать, что инцидент нарушения безопасности — это то, что запрещено законами конкретной страны.

— **Получается, что с такими вещами каждый сталкивается ежедневно... Но ведь не всё, что запрещено, столь уж опасно?**

— (Байба) Да, я думаю, что около 90—95% таких угроз скорее надоедливы, они не очень угрожают в прямом виде. Другое дело оставшиеся пять процентов: здесь уже речь идёт о чём-то, что может повлечь потерю ресурсов, в том числе и денежных.

— **Подожмите, но ведь пиратское ПО тоже запрещено законом, а значит, тоже является таким инцидентом?**

— (Артур) Если мы говорим о конечных пользователях, то у них это обычно выражается в использовании различных файлообменных программ. Максимум, что может сделать провайдер — закрыть доступ. Хотя можно привлечь и полицию.

(Байба) Да, легальность ПО — это не наш профиль, этим



■ Артур Меденис: "Говоря о нарушениях, наше дело — не столько наказать "чужого", сколько защитить "своего" и сделать невозможным повторение такого же инцидента".

занимаются другие организации, например, BSA. Мы намерены концентрироваться на повышении образованности пользователей и решении самих проблем, равно как и борьбе со спамом.

— **А можно ли за спам схлопотать реальный срок в нынешних условиях?**

— (Артур) Закон об этом есть, но реально не работает. До суда дело на моей памяти ни разу не доходило — это слишком сложно доказать. В нужный момент всегда появится адвокат, который убедит судью в том, что человек это делал не сам, его машину заразили и всё сделали за него. И вообще, если говорить начистоту — в Латвии есть только один судья, который разбирается в вопросах, связанных с IT-технологиями.

(Байба) Да и вообще, отделить спам от не спама очень непросто. И определение спама как нежелательной корреспонденции тоже совершенно не помогает. Любая фирма, разместившая где-либо контактный e-mail, вряд ли имеет право предъявить претензии, если им идёт какая-то реклама. Ведь они сами просили присылать им различную информацию!

(Артур) Да, но если какая-то реклама приходит по десять раз в день — это уже определённно спам. Особенно, если получатель явным образом просил больше не присылать ничего подобного.

— **Наверное, спам и правда можно только терпеть, бороться с ним сложно. Но как насчёт других проблем — как можно решить их?**

— (Байба) Уменьшить число инцидентов нарушения безопасности можно, в первую

очередь, с помощью повышения грамотности пользователей. Но, с другой стороны, постоянно придумывают что-то новое — поэтому и получается, что такие проблемы будут всегда. Провайдеры могут пробовать только защитить своих клиентов. Например, перекрывать доступ в сеть внешним пользователям, за которыми ранее было замечено что-то нехорошее. Кроме того, можно попытаться связаться с провайдером нарушителя, чтобы он тоже принял какие-то меры.

— **А как успехи с местными поставщиками услуг интернета?**

— (Артур) У нас есть контакт со многими провайдерами, некоторые более отзывчивы, некоторые — менее.

(Байба) Такое взаимодействие началось недавно, потому говорить о конкретных результатах пока рано. Но в любом случае значительно тормотит прогресс то, что даже в крупных компаниях далеко не всегда есть люди, которые занимаются исключительно инцидентами нарушения безопасности. А значит, времени на решение таких вопросов остаётся очень мало. К тому же, на этом толком и заработать не получится, да и оценить эффективность таких мер тоже непросто.

— **Быть может, нужно более агрессивно (в хорошем смысле этого слова) убеждать всех в необходимости заботиться таким образом о своих же клиентах?**

— (Артур) Конечно, но там ведь всё намного проще доказать — просто конфискуется техника, а потом уже смотрят, есть ли там что-то нелегаль-



■ Байба Кашкина: "Надеюсь, что в нашей стране найдутся люди, которым небезразлична безопасность латвийского интернета и которые будут предпринимать конкретные действия. Например, создавать CERT-группы или хотя бы участвовать в местном CERT-движении".

— (Байба) Мы никому не хотим ничего навязывать! На мой взгляд, в данном случае нужно заинтересовать людей, но никак не заставлять. К тому же, у нас нет никакой законодательной или иной власти — так что ни реально наказать виновных, ни заставить всех провайдеров принимать какие-то меры мы просто не можем.

(Артур) Да, говоря о нарушениях, наше дело — не столько наказать "чужого", сколько защитить "своего" и сделать невозможным повторение такого же инцидента.

— **Когда-то и BSA тоже действовала сама по себе, и все мы знаем, в какую силу она превратилась сейчас...**

— (Артур) Конечно, но там ведь всё намного проще доказать — просто конфискуется техника, а потом уже смотрят, есть ли там что-то нелегаль-

ное или нет. А пользователь интернета в любом случае может заявить, что атаку делал не он, что его тоже взломали и т. д.

— **И с чего же нужно начать, кто должен быть заинтересован в создании похожих групп?**

— (Байба) В первую очередь, это провайдеры. И крупные организации, те же банки. Ведь у них тоже есть очень большие сети, и они заинтересованы в их безопасности. Думаю, будут необходимы и кампании при поддержке правительства — такое было и в Литве, и в Эстонии.

(Артур) Причём на мой взгляд здесь сработало бы нечто запугивающее. Помните кампании против пьяных водителей и пешеходов без отражателей? Быть может, здесь тоже должно быть что-то подобное.

(Байба) Да, и запугивать нужно не только перспективных нарушителей. Многие пользователи просто не осознают, насколько серьёзна ситуация, например, в случае интернет-банка, не могут понять, что их кошелек уже не в кармане, а в Сети. А значит, к нему, в принципе, может получить доступ человек из любой страны мира — если не предпринимать определённые меры предосторожности.

Но в любом случае, надеюсь, что в нашей стране найдутся люди, которым небезразлична безопасность латвийского интернета и которые будут предпринимать конкретные действия. Например, создавать CERT-группы или хотя бы участвовать в местном CERT-движении. Мы готовы сотрудничать со всеми, кто хочет сделать интернет безопаснее, и с радостью поможем советами.

— **Спасибо за беседу!**

ЕСТЬ МНЕНИЕ

Алексей ТАРАСОВ alexey.tarasov@times.lv

Лишняя головная боль

Быть может, пока слишком рано говорить о том, какова же судьба CERT-групп в ближайшем будущем Латвии. Как человек, которому небезразлична судьба латвийской части интернета, я целиком "за" подобные инициативы. Корпоративные клиенты и крупные поставщики услуг интернета платить за такое будут вполне готовы — в их области за безопасность действительно готовы отдать сколько угодно. Но попытаемся взглянуть на проблему с точки зрения домашних пользователей и провайдеров.

Представим себе среднего статистического домашнего провайдера, который при этом предоставляет действительно качественный сервис.

Не секрет, что бизнес этот — не то, чтобы очень прибыльный. И тут придётся создавать специальную структуру, которая ещё и не будет напрямую окупаться. Захочет ли провайдер повышать и без того небольшие цены, ведь кто-то должен будет оплачивать эти дополнительные услуги? Скорее всего, нет. И это не значит, что о безопасности он не думает — он просто ограничивается мерами вроде брандмауэров, спам-фильтров на стороне сервера и т. д. Не хочется терять клиентов, приносящая их платить больше. А пользователь сейчас всё-таки смотрит на цену. Ему не столь принципиально, что у провайдера X безопаснее, если он берёт вдвое больше, чем про-

вайдер Y. И с большой вероятностью человек выберет более "доступный" вариант.

Так что добровольно домашние поставщики услуг интернета вряд ли согласятся создавать какие-то CERT-подразделения. Им и так выжить очень и очень непросто, тем более, не хочется терять клиентов. Поэтому самой действенной мерой борьбы с различными опасностями пока является именно просвещение пользователя, о котором говорила госпожа Кашкина. Но ждать, что в это дело сразу включится много организаций, мы, пожалуй, не станем. Наверняка, этот процесс рано или поздно начнётся, вопроса всего два. Первый — "когда именно?", а второй — "кто за всё заплатит?". Подключить бы сюда какие-нибудь еврофонды...



Стабильный сервер, надёжно защищающий данные за приемлемую цену



Найдешь по адресу: www.hp.lv/server

HP ProLiant DL360 G5
Двухъядерный процессор Intel® Xeon®



© 2007 Hewlett-Packard Development Company L.P. Все права защищены. Intel, Intel logo, Intel Inside, Intel Inside logo, Xeon и Xeon Inside являются торговыми марками или зарегистрированными торговыми марками Intel Corporation или дочерних компаний в США и других странах.