АНДРЕЙ ВЛАДИМИРОВ

УШЕЛ В IT ИЗ «ЧИСТОЙ» НАУКИ, ТАК КАК «ТАМ НЕ ДАЮТ ЗАНИМАТЬСЯ ЧЕМ ХОЧЕШЬ». СПЕЦИАЛИЗИРУЕТСЯ В ОСНОВНОМ НА БЕЗОПАСНОСТИ СЕТЕВОЙ ИНФРАСТРУКТУРЫ: МАРШРУТИЗАТОРЫ, КОММУТАТОРЫ, ТОЧКИ ДОСТУПА И Т.Д. РАБОТАЕТ С ПРОТОКОЛАМИ НА НИЖНИХ УРОВНЯХ: КАНАЛЬНЫЙ, СЕТЕВОЙ, БЕЗОПАСНОСТЬ КОММУТАЦИИ И МАРШРУТИЗАЦИИ

КОНСТАНТИН ГАВРИЛЕНКО

СПЕЦИАЛИСТ С ОПЫТОМ РАБОТЫ В СФЕРЕ ИТ-БЕЗОПАСНОСТИ БОЛЕЕ 12-ТИ ЛЕТ. СОАВТОР ДВУХ КНИГ: «WI-ФУ: СЕКРЕТЫ БЕСПРОВОДНОГО ВЗЛОМА» И «СЕКРЕТЫ ХАКЕРОВ: БЕЗОПАСНОСТЬ СЕТЕЙ CISCO»

АНДРЕЙ МИХАЙЛОВСКИЙ

БОЛЕЕ ДЕСЯТИ ЛЕТ АКТИВНО ЗАНИМАЕТСЯ СЕТЯМИ, СИСТЕМАМИ АУТЕНТИФИКАЦИИ, БЕСПРОВОДНОЙ СВЯЗЬЮ, КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТЬЮ И УЧАСТВУЕТ В РАЗРАБОТКАХ И ИССЛЕДОВАНИЯХ КОМПАНИИ «АРХОНТ»

проверено электроникой

АУДИТОРЫ БЕЗОПАСНОСТИ

ОНИ АВТОРЫ НЕСКОЛЬКИХ ПОПУЛЯРНЫХ КНИГ ПО БЕЗОПАСНОСТИ, МНОГОЧИСЛЕННЫХ ПУБЛИКАЦИЙ ОБ ОБНАРУЖЕННЫХ УЯЗВИМОСТЯХ НА ФОРУМАХ И СЕТЕВЫХ РЕСУРСАХ (BUGTRAQ, PACKETSTORM, SECURITYLAB), А ТАКЖЕ В ПРЕССЕ (LINUX WORLD, LINUX MAGAZINE, INFORMATION SECURITY AUDITOR, INTERNET WORLD, THE BYTE). ОНИ РУССКИЕ :), НО БАЗИРУЮТСЯ В АНГЛИИ. С НИМИ МЫ И ПОБЕСЕДОВАЛИ... |**АНДРЕЙ КАРОЛИК (ANDRUSHA@REAL.XAKEP.RU)**

СПЕЦ: НАСКОЛЬКО СЛОЖЕН ПУТЬ ОТ ВОЗНИКНОВЕНИЯ ИНТЕРЕСА К БЕЗОПАСНОСТИ ДО ОБРАЗОВАНИЯ ЦЕЛОЙ КОМПАНИИ?

КОНСТАНТИН ГАВРИЛЕНКО: В сфере инфосека самое простое — основать и организовать свое дело, в первую очередь — начать продавать сервисы и свои знания: для этого не нужно дорогостоящее оборудование, помещения и т.д. Соответственно, затраты на организацию несоизмеримо меньше. Начинали скромно, у каждого по десктопу, выход в интернет :). Потом прикупили несколько лаптопов (для беспроводных сетей), пару маршрутизаторов, и так до пары раков с оборудованием. Когда мы открывались, про нас вообще никто не знал, все мы пришли из сфер, не связанных с ИТ, поэтому пришлось достаточно много времени потратить на наработку связей в индустрии, какой-то известности, доверительных отношений с клиентами. Стереотип «русских хакеров» часто проявлял себя как незаменимый, а иногда наоборот...

АНДРЕЙ МИХАЙЛОВСКИЙ: Поскольку «Архонт» небольшая компания, приходится выполнять разносторонние обязанности от общения с клиентами до высокотехнических сфер. И буквально через год после открытия компании о нас знали на разных компьютерных выставках и конференциях, а еще через год вышла первая книга — «Wi-Foo: the Secrets of Wireless Hacking». Чем больше мы узнавали рынок, тем сильнее убеждались в своих способностях в области компьютерной безопасности. Как показала практика, реальных специалистов в этой сфере не так уж много.

АНДРЕЙ ВЛАДИМИРОВ: Все зависит от величины интереса. Главное — иметь команду, которая способна выполнять разносторонние функции, чтобы участники были активны и желали привнести что-нибудь свое в работу компании. А в плане рынка — иметь свою нишу, причем нужно искать ее как раз не из-за узконаправленности предоставляемых услуг, а скорее наоборот. Не быть привязанным к одному производителю, системе методологий или решению, а предоставлять клиенту выбор с оценкой оптимума, учитывая его специфические требования и бюджет. Как говорится, клиент всегда прав.

СПЕЦ: ПОЧЕМУ АНГЛИЯ? ЧЕМ ЛУЧШЕ УЧЕБА ТАМ? ЧЕМ ЛУЧШЕ РАБОТА? У НАС НЕТ ПЕРСПЕКТИВ?

КОНСТАНТИН ГАВРИЛЕНКО: Вообще-то я из Риги :). Так уж получилось, что учиться пришлось в Англии. Сначала школа, потом институт, потом магистратура. На момент окончания обучения я провел в Англии семь лет, успел адаптироваться и обзавестись друзьями и контактами. К тому же была идея открытия своего бизнеса, а нглийский рынок для этого подходил, то есть вопрос решился сам собой. Дополнительное «за» состояло в том, что мы все были не только из разных городов бывшего Советского Союза, но даже из разных республик, а на сегодня — еще и из разных государств. Переезд куда-то на новое место жительства означало то, что придется начинать все заново, с нуля.

В России все только начинается, рынок потихоньку движется в правильном направлении, и потенциал развития просто огромный. Основная проблема, на мой взгляд, в том, что менеджмент компаний еще не осознал важность направления информационной безопасности, связанные с этим потенциальные убытки, что основная ответственность ложится на них и что это не работа для простого админа/компьютерщика. Факультет ВМК МГУ и профессор Сухомлин работают в правильном направлении, и, возможно, с нашей помощью в скором времени появится отдельная программа по подготовке специалистов по ИТ-безопасности.

АНДРЕЙ МИХАЙЛОВСКИЙ: Я бы не сказал, что в Англии учеба лучше, чем в России, скорее наоборот. Система образования в этой стране основана на узкой специализации учеников, что в конечном итоге ограничивает сферу знания и интересы людей. Я выбрал Англию из-за ее репутации на международном уровне. Ведь многие на западе считают Россию коррумпированной страной, с распространенным взяточничеством, что, в свою очередь, негативно сказывается и на образовании. К тому же менеджмент и бизнес-науки в Англии преподаются лучше, так как в европейских вузах в этой сфере накоплено больше опыта.

К сожалению, коммерческий рынок ИТ-безопасности в России практически не существует и, можно сказать, опаздывает минимум на пять лет по сравнению с Европой, Азией и Америкой. На российском рынке специалисты по безопасности не пользуются популярностью, к тому же совсем не многие фирмы могут выделить из бюджета по $2 000 в день на эти услуги, что по европейским стандартам считается нормой.

АНДРЕЙ ВЛАДИМИРОВ: Чем больше живу, тем тверже убеждаюсь в том, что «свобода выбора» — всего лишь миф. Если, конечно, твоего отца зовут не Билл Гейтс. В моем конкретном случае, на момент переезда в Англию «выбор» был: либо принимать предложенный грант от Лондонского университета, либо буквально жить на улице. В моей лаборатории (а я тогда работал в биотехе) просто-напросто закончились реактивы, животные, не было доступа к последним публикациям на изучаемые темы. Союз окончательно развалился, исследователи в республиках СНГ (в данном случае на Украине) оказались просто-напросто никому не нужны.

А в России перспективы, безусловно, есть. Приезжаю время от времени читать курсы в АИС в Москве. Появляемся с докладами на российских конференциях. Со временем, очевидно, откроем свое представительство в России и, в принципе, мы полностью открыты предложениям отечественных компаний...

СПЕЦ: КОМПАНИЯ — ВСЕГО ШЕСТЬ ЧЕЛОВЕК. ЧТО ВЫ МОЖЕТЕ? ЕСТЬ ГИГАНТЫ, ШТАТ В НИХ НАСЧИТЫВАЕТ СОТНИ СПЕЦИАЛИСТОВ...

КОНСТАНТИН ГАВРИЛЕНКО: В данном случае важно не количество, а качество. В последнее время появилось достаточно много контор по безопасности, которые используют пару-тройку различных коммерческих сканеров и выдают их за полноценный аудит безопасности, что формирует у потребителя ложное чувство обеспеченности безопасностью. В плане диверсификации у каждого участника команды есть своя зона ответственности, потом складывается общий результат работы. Конкурентоспособность в основном достигается за счет качества выполненной работы.

АНДРЕЙ МИХАЙЛОВСКИЙ: Для проверки безопасности не обязательно иметь большой коллектив работников: чем больше людей работают над проектом, тем тяжелее организовать и собрать нужную и детальную информацию, прийти к конкретному решению задачи. Оптимально — четыре-шесть человек в команде для получения результативного аудита большинства средних и крупных компаний.

Работая с клиентами, мы всегда смотрим на безопасность с позиций потребителя, полностью учитываем структуру предприятия-клиента, сферу деятельности и его потребность в компьютерной безопасности. Мы никогда не навязываем какой-то одной компании сервис, решение или оборудование. Наоборот, предлагаем выбор и подробно оцениваем кандидатуры. Большинство наших конкурентов для аудита используют решение или программное обеспечение той или иной компании, тем самым ограничивая себя и предоставляемый сервис. Мы стараемся смотреть на безопасность со всех сторон, использовать как можно больше оборудования и утилит, при этом проверяем и анализируем каждый полученный результат. В этом одно из главных наших отличий от конкурентов, которые проводят автоматизацию не-

обдуманно, прогоняют коммерческий сканер или программу, распечатывают отчет и считают, что аудит безопасности на этом закончен.

АНДРЕЙ ВЛАДИМИРОВ: Вспоминается старый анекдот о сравнении нашей и японской корпораций, он заканчивается на фразе «Вот никак не поймем, что же делает здесь 501-й сотрудник». Множество сотрудников в больших компаниях — балласт, особенно в консультационных компаниях. У нас балласта нет, и отбор людей весьма тщательный, он не зависит от личных симпатий и антипатий. На крайний случай под рукой есть проверенные специалисты для привлечения к выполнению отдельных заданий на контрактной основе. Кстати, сколько сотрудников было в Microsoft году так в 77-м?

Мы можем многое. Практически любая операционка, любой уровень OSI и сетевой протокол, любая топология сети... Конкуренты же в этом плане часто отстают. К примеру, во многих фирмах методология проведения внутренних и внешних аудитов сетей ничем не отличаются. Беспроводные сети нормально не покрыты. Не уделяется внимания протоколам на канальном уровне. Нет уровня экспертизы, позволяющего находить новые уязвимости, есть жесткая привязка к отдельным решениям специфических производителей. И так далее...

СПЕЦ: ЧТО НАИБОЛЕЕ АКТУАЛЬНО СЕГОДНЯ? ЧЕМ ЖИВУТ СОВРЕМЕННЫЕ ЭКСПЕРТЫ ПО БЕЗОПАСНОСТИ?

КОНСТАНТИН ГАВРИЛЕНКО: Мир инфосека слишком динамичен, чтобы какая-то определенная область оставалась актуальной долгое время. Наиболее уязвимы новые технологии, которые еще не проверены временем, или технологии, набирающие популярность. Последние пару лет все без исключения конторы по безопасности демонстрируют способы проникновения через уязвимости в web'е. Складывается такое впечатление, что кроме SQL-инъекции и седьмого уровня, больше ничего не существует. К сожалению, это не так, и при оценке безопасности сетевой инфраструктуры многие вещи остаются незамеченными, что мы неоднократно видели, проверяя работу других «экспертов». В плане security-оборудования, на мой взгляд, стоить обратить внимание на системы предотвращения вторжения (IPS), web-брандмауэры (Layer-7 firewall), SSL виртуальные частные сети (SSL VPN) и системы централизованного управления беспроводными сетями.

АНДРЕЙ ВЛАДИМИРОВ: Защита инфраструктуры сетей: коммутаторов, маршрутизаторов и т.д. Им должно уделяться не меньше внимания, чем серверам. Беспроводные сети всех типов. Мобильные устройства и их встроенные операционные системы. Web-приложения. Базы данных. Системы предотвращения вторжений (IPS), защита клиентских устройств на уровне ядра системы и системных вызовов, концепция «самозащищающихся» сетей. «Умная» и действенная фильтрация спама и вредоносных программ. В отдельных областях (интернет-магазины, аукционы, казино и букмекеры) — DDoS-атаки и эффективная защита от них.

СПЕЦ: ВАМИ НАПИСАНО СТОЛЬКО КНИГ И СТАТЕЙ... КОГДА ЖЕ УСПЕВАЕТЕ РАБОТАТЬ?

КОНСТАНТИН ГАВРИЛЕНКО: Спим мало :), да и то обычно перед компьютером. Вся информация в книгах, статьях о новых уязвимостях — это наработки, сделанные за время проведения аудитов. А само написание после проделанных исследований занимает не так уж и много времени. Главное — это стремление познать что-то новое, найти новые методы решения задач.

АНДРЕЙ МИХАЙЛОВСКИЙ: Смотря что называть работой. Для нас и других специалистов в сфере компьютерной безопасности работой может считаться почти все что угодно — от конфигурации программы или девайса, проверки протоколов и стандартов до программирования и создания кода и эксплойтов. Большую часть времени мы проводим перед компьютерами, читая документации, статьи и публикации, играясь с различными программами и оборудованием.

СПЕЦ: ЕСТЬ ЛИ КАКИЕ-ТО НОУ-ХАУ В ОБЛАСТИ БЕЗОПАСНОСТИ, КОТОРЫЕ ВЫ СОЗДАЛИ САМИ?

КОНСТАНТИН ГАВРИЛЕНКО: Конечно, есть. Взгляни на лист опубликованных найденных уязвимостей :). Кроме того, наша методология оценки безопасности и проникновения в беспроводные сети, опубликованная в аппендиксе к «Wi-фу», была первым систематизированным документом на эту тему. В плане утилит… Мы в основном используем ПО с открытым кодом, поэтому не только берем, но и отдаем взамен для общего блага. Например, на данный момент единственной утилитой, способной генерировать произвольные пакеты для EIGRP-протокола маршрутизации, является наша EIGRP-tools. Примечательно, что все наши утилиты включены в различные дистрибутивы для оценки безопасности, значит, время было потрачено не зря.

АНДРЕЙ МИХАЙЛОВСКИЙ: «Архонт» разработал несколько образцов и шаблонов для проверки безопасности беспроводных сетей, которыми пользуются многие консультанты и коммерческие организации в нашей индустрии. Мы также создали шаблоны для анализа оборудования, программ и стандартов с проприетарным кодом. Во время написания Hacking Exposed «Архонт» разработал методы и утилиты для проверки безопасности оборудования и протоколов, использованных компанией Cisco при распределении трафика в интернете.

АНДРЕЙ ВЛАДИМИРОВ: Разумеется, есть, и кое-что надо будет даже запатентовать. А информацию насчет обнаружения новых уязвимостей и написания утилит с открытым кодом для «общественного пользования» ты всегда можешь найти на наших сайтах: **www.arhont.com**, **www.wi-foo.com** и **www.hackingciscoexposed.com**