Взламываем Хакера

Часть III

Учимся у экспертов борьбе с хакерами

Роджер А. Гримс

Перевод: @Samigg
http:\\skladchik.com

Глава 33. Сетевые атаки

В Главе 2, “Как Хакеры Взламывают”, мы обсудили различные способы взлома компьютеров. Мы рассмотрели физические атаки, уязвимости нулевого дня, непропатченное ПО, социальная инженерия, слабые пароли, прослушка/атаки man-in-the-middle, утечка данных, неправильная настройка, DoS-атаки, ошибки пользователей и вредоносное ПО. Все эти методы взлома могут быть использованы как против самого компьютера, так и против сети, к которой он подключен.

Виды Сетевых Атак

Сетевые атаки могут применяться на любом уровне сетевой модели OSI (Open Systems Interconnection) (https://en.wikipedia.org/wiki/OSI_model). Модель OSI - наиболее распространенный стандарт взаимодействия открытых систем, где есть несколько уровней, на которых могут взаимодействовать системы. В модели OSI семь уровней:

- Физический
- Канальный
- Сетевой
- Транспортный
- Сеансовый
- Представительский
- Прикладной

Взлом сети, а также устройств управления сетями, может осуществляться на всех уровнях (сетевые устройства так же могут запускать приложения), при этом взлом компьютера в сети также может осуществляться на многих уровнях. Атака на физическом уровне осуществляется путем получения доступа, поломки или кражи сетевого оборудования. Для атак на канальном уровне используются сетевые мосты, коммутаторы, а также протоколы и стандарты этих уровней, например, MAC-адрес устройства (https://en.wikipedia.org/wiki/MAC_address). Сетевой уровень отвечает за маршрутизацию. Транспортный и сеансовый обеспечивают передачу данных на верхние уровни, а прикладной и представительский отвечают за отображение данных на устройстве или в приложении. Если в сетевой среде передачи

данных работает несколько пользователей, и нет дополнительной защиты, то всегда есть вероятность, что один узел сети может вмешиваться в работу других узлов. В следующих разделах описаны самые популярные виды сетевых атак.

Прослушка

Прослушка - несанкционированный просмотр и/или запись частной беседы. Хотя сейчас этот метод не является таким успешным, раньше можно было использовать анализатор трафика, с помощью которого можно было увидеть в открытом виде запись разговоров или учетные данные. В интернете существует огромное количество бесплатных инструментов, которые можно скачать, нажать одну кнопку и начать перехватывать пароли в открытом виде. Так же есть инструменты для перехвата cookies и сессий. Как правило, для работы с такими программами не требуются особые знания, их нужно просто запустить и все будет работать.

Атаки Man-in-the-Middle

MitM-атаки (Man-in-the-middle, "человек посередине") также могут осуществляться на любом уровне модели OSI. Используя такую атаку, злоумышленник незаконно проникает в канал связи между несколькими авторизованными сторонами, притворившись одной из них. При этом та сторона, которой притворяется злоумышленник, как правило, исключается из этого канала. MitM-атаки используются с той же целью, что и прослушка, их используют для просмотра и кражи личных данных. Однако, эти атаки также используются для модификации сообщений и данных, например, ответ "нет" вместо "да", или для перенаправления одного или нескольких участников на сторонний ресурс.

Сегодня, многие приложения и протоколы имеют встроенные средства защиты от MitM-атак, однако эти средства не всегда включены по умолчанию, довольно часто так происходит из-за опасений потери производительности или несовместимости. Например, бесплатная технология DNSSEC была разработана в 2004-ом для предотвращения DNS-спуфинга (DNS spoofing), но спустя огромное количество времени ее по-прежнему используют менее 1% DNS-серверов во всем мире.

DDoS-атаки

DDoS-атаки, вероятно, являются самыми распространенными и, совершенно точно, наиболее частыми в интернете. Каждый день терабайты данных

отправляются с целью помешать работе различных сайтов и сервисов. DDoS-атаки могут использоваться на любом уровне модели OSI.

Способы Защиты от Сетевых Атак

Существует множество способов защиты от сетевых атак, некоторые из них, описаны в следующих разделах.

Изоляция Домена

Изоляция домена - это создание безопасной границы, отделяющей разрешенный трафик от нежелательного. Для реализации этого подхода существует множество инструментов и методов, включая файрволы, виртуальные частные сети, IPSEC, роутеры, программно-определяемые сети (SDN, software-defined networks) и т.д. Как правило, если сетевая атака не может достичь устройства или сети, то она не сможет навредить. Существуют пограничные случаи, когда DDoS-атака может повлиять на зависимые объекты, и, таким образом, достичь своей цели. Но, в любом случае, изоляция домена принесет только пользу.

Виртуальные Частные Сети

Виртуальная частная сеть (Virtual Private Network, VPN) - одно из лучших решений при работе в открытых сетях общего использования. Технология VPN может быть реализована с помощью программных и аппаратных компонентов или их сочетания. Как минимум, VPN шифрует весь трафик между отправителем и, по крайней мере, первым узлом, а иногда и на всем пути передачи данных. VPN не идеальны. Например, DDoS-атака может прервать работу VPN.

Использование Безопасных Протоколов и Приложений

Нет ничего лучше безопасного протокола и приложений, которые защищены от известных угроз. Если есть такая возможность, то нужно использовать безопасные протоколы и приложения (такие, как SCP и SSH) и стараться не использовать известные небезопасные протоколы (такие, как FTP и Telnet). Также, ни одно приложение не должно хранить учетные данные в открытом виде на диске, в памяти, или передавать их по сети.

Обнаружение Вторжения в Сеть

Сетевые атаки могут быть обнаружены с помощью снифферов (вручную) или с помощью механизмов поиска определенных шаблонов вредоносных действий. Если вредоносная активность будет обнаружена, то она может быть остановлена, или пользователь получит оповещение безопасности с выбором действия. Анализаторы сетевых протоколов (такие, как снифферы) - это отличный инструмент для перехвата и расшифровки причин сетевых аномалий. Снифферы позволяют анализировать трафик как вручную, так и в автоматическом режиме. Многие файрволы также имеют встроенные средства обнаружения вторжений.

Средства Защиты от DDoS-атак

Защититься от DDoS-атак можно с помощью усиления защиты сетевого оборудования, расширения пропускной способности сети, а также используя специальные сервисы. Сегодня существуют десятки сервисов, способных защитить компании от масштабных DDoS-атак. Единственная проблема в том, что их услуги достаточно дороги, и порой проблему создают именно поставщики такого сервиса. К сожалению, есть немало неэтичных конкурентов, которые пойдут на все, чтобы переманить клиентов к себе. Если вы хотите использовать сервис, предоставляющий защиту от DDoS-атак, проведите собственное расследование. Только так вы сможете убедиться в надежности и этичности этой компании.

Посещение Безопасных Веб-сайтов и Использование Безопасных сервисов

Многие сетевые атаки, такие как кража cookies или данных аутентификации происходят только потому, что при создании этих веб-сайтов или сервисов не используется Security Development Lifecycle (SDL). Веб-сайт или сервис, который был правильно написан, прошел моделирование угроз, а также использует SDL для устранения известных уязвимостей, гораздо более устойчив к сетевым атакам.

К сожалению, обычному интернет-пользователю трудно понять, применяются ли на данном веб-сайте или в веб-сервисе безопасные методики программирования. Некоторые веб-сайты прошли аттестацию известных поставщиков решений в сфере безопасности, и, если на сайте есть их аттестат, то обычный пользователь, как правило, чувствует себя комфортнее.

Сетевые атаки в интернете случаются каждый день, и некоторые из них, наносят огромный урон своим жертвам. Существует множество средств защиты

от сетевых атак, которые могут принести выгоду пользователям и организациям, снизив риск воздействия атаки.

В следующей главе мы поговорим о Лоре Чаппелл, одном из лучших специалистов в области анализа сетевого трафика.

Глава 34. Профиль: Лора Чаппелл

Ученые говорят, что если мы когда-нибудь встретим инопланетную цивилизацию, то, вероятнее всего, языком для общения будет математика, потому что математика - это действительно единственный язык во вселенной, который будет понятен более развитой цивилизации. Единственный способ понять, что происходит с компьютером, подключенным к сети - проанализировать трафик. Никто не делает это лучше, чем Лора Чаппелл. Она как Луиза Бэнкс (которую сыграла Эми Адамс) из фильма 2016 года *Прибытие* или Элли Эрроуэй (которую сыграла Джоди Фостер) из фильма 1997 года *Контакт*. Она очень умная, сосредоточенная, особенно хороша в своем деле, и уважаема среди коллег.

Ее лекции и презентации всегда собирают много людей, и высоко ими ценятся. Впервые, я встретился с ней 20 лет назад, когда она вела лекцию для местных IT-специалистов по сниффингу в Вирджиния-Бич, штат Виргиния. В то время в IT-индустрии было мало женщин, и Чаппелл привыкла к нападкам парней из этой индустрии, которые хотели показать, что знают больше о перехвате пакетов. Она закончила вступительную речь, сказав нашей группе: "Если думаете, что можете выйти сюда и впечатлить меня своими знаниями альфа-самца о перехвате пакетов, это будет пустая трата времени. Я знаю больше вас". Аудитории это понравилось. Затем она доказала, что была права, и мы стали ее преданными фанатами.

Она пользовалась практически всеми снифферами пакетов, хотя сейчас ей больше всего нравится популярный Wireshark (http://www.wireshark.com), у которого существует как бесплатная, так и платная версии.

Я спросил Чаппелл, почему ее заинтересовал анализ пакетов, она ответила: "В конце 1980-ых и начале 1990-ых я работала в Novell (в то время эта компания была локомотивом сетевых операционных систем). Я была в Novell Technology Institute, в команде гиков, которые проводили исследования, писали и вели лекции на самые горячие в то время темы о сетевых технологиях. Когда в 1989-ом Рей Нурда, главный исполнительный директор Novell, купил Excelan Corporation, мне посчастливилось оказаться на презентации Excelan LANalyzer. Наблюдая за тем, как эта ранняя программа анализа трафика подключалась к сети Novell, разбирала запросы/ответы, высвечивала на экране сообщения с именами пользователей и паролями в заголовке… я увлеклась! Я сказала себе (и всем, кто сидел рядом и слушал) "Я хочу заниматься этим всю свою жизнь". Боже… И вот, спустя все эти годы, я все еще анализирую данные в сети!".

Я спросил Чаппелл, как она попала в сферу информационной безопасности. Она сказала: "Впервые, я начала проводить расследование сетевой атаки по воле случая. В 1993-ем, я открыла свою компанию и проводила большую часть времени, анализируя сети различных корпораций на местах. Тогда лишь немногие компании были заинтересованы в решение проблем, оптимизации и планировании пропускной способности. Тогда никто не звал меня поговорить о "безопасности".

Однако, в течение многих лет работы, я подключалась к инфраструктуре компании только для того, чтобы обнаружить огромные проблемы безопасности во всей их сети. Не упуская из виду основную задачу, которая интересовала клиентов, я стала доводить до них информацию о проблемах безопасности. Я видела пакеты и запросы в их сети, которых просто не должно было быть. Было немало случаев, когда я понимала, что плохая работа сети была *наименьшей* из их проблем - их грабили прямо у них под носом (точнее по проводам). Стало очевидно, что мне нужно добавить "анализ безопасности" к моим обычным задачам сетевого анализа. Расследование сетевых преступлений стало первоочередной задачей. Вот несколько наглядных примеров:

Посреди анализа плохо работающей сети клиента на месте, я обнаружила внезапный, безостановочный поток трафика, который направлялся к точке выхода из сети. Этот трафик исходил от системы, которая должна быть относительно тихой, так как на этой машине никто не работал. Присмотревшись внимательнее к этому потоку трафика, я обнаружила в нем множество знаков доллара и большие суммы в долларах. После воссоздания этого потока, я поняла, что у меня есть абсолютно все платежные ведомости компании.

Во время анализа сети в больнице я обнаружила, что, студенты из крупного университета, по всей видимости, получили доступ к рецептурной базе данных, в которой содержались не только имена, адреса и номера соцстрахования пациентов, но также полное описание выписанных медикаментов, и причины, по которым их выписывали. Моей первоочередной задачей был анализ сессий, необходимо было обнаружить причину медленной авторизации. Однако, после того, как я обнаружила подозрительный трафик, все изменилось. Я стала заниматься обнаружением вредоносного трафика". Остальное уже история.

Я спросил Чаппелл, что сейчас представляет для нее наибольший интерес в сфере информационной безопасности. Она сказала: "Это сложный вопрос. Существует так много увлекательных направлений расследования сетевых атак. Два, наиболее интересных мне сейчас: Обнаружение автоматических фоновых процессов, когда они отправляют конфиденциальную и личную информацию незаметно для пользователей, и обучение ребят настройке Wireshark, чтобы они могли быстро обнаружить основные признаки разведки сети и атаки на нее. Я считаю настройку Wireshark горячей темой. Конфигурация Wireshark,

которая быстро сообщит оператору об угрозе - это очень полезный инструмент. Мне очень нравится учить ребят пользоваться Wireshark'ом для анализа сети".

Я спросил, что она считает самой большой проблемой информационной безопасности. Она ответила: "Исходя из опыта расследования сетевых преступлений, я должна сказать, что немногие компании понимают, как должны взаимодействовать различные подразделения. Мой опыт показывает, что ребята, которые устанавливают ПО на компьютеры организации, не заинтересованы в изучении безопасности сети - они просто устанавливают ПО и все. Они не проводят анализ трафика к/от недавно установленной системы. Они не понимают, как выглядит "нормальный" трафик, поэтому они не могут определить если он ненормальный. У них точно нет доступа к IDS-системе, они не пропускают через нее файлы трассировки. Было бы замечательно, если бы ребята, занимающиеся безопасностью в компаниях, проводили обучение о способах взлома системы и том, как предотвратить проблемы в будущем. Я знаю, у этих ребят много работы, но им нужно делиться знаниями с другими подразделениями".

В конце интервью, я спросил, что она порекомендовала бы тем, кто рассматривает карьеру в информационной безопасности. Она ответила: "Конечно же, во-первых, необходимо выучить Wireshark! Шучу… хотя нет, на самом деле, не шучу. Wireshark - это идеальный инструмент для изучения работы сети, и он бесплатный! Не зря это инструмент безопасности №1 по версии sectools.org (Серьезно, наблюдать за рукопожатием (handshake) TCP намного интереснее, чем читать о нем в RFC!).

Во-вторых, очень, очень хорошо знать TCP/IP. Уделите время перехвату собственного трафика при подключении к веб-серверу, отправке электронного письма, загрузке файла на FTP, и так далее. Пока вы изучаете, как работают протоколы, *наблюдайте* за их работой, используя Wireshark. Наблюдайте за тем, как работает рукопожатие в TCP, за природой запроса/ответа при работе приложений, как происходит процесс разъединения, и так далее.

В-третьих, соберите небольшую лабораторию для проведения атак. Не обязательно, чтобы компьютеры были дорогими и мощными, просто объедините несколько компьютеров через коммутатор и используйте бесплатные инструменты для сканирования/тестирования на проникновение. Во время проведения атак на свои системы, перехватывайте и анализируйте трафик. Большинство из нас лучше воспринимают наглядную информацию - смотреть, как работает сеть намного интереснее, чем просто читать о том, как все происходит. Информационная безопасность включает две стороны одной медали. Необходимо видеть и понимать, как работают различные атаки, только так можно понять, как от них защититься.

Это игра. Игра в "найди решение проблемы" - это отличный способ натренировать мозг для анализа сети и безопасности.

Лора Чаппелл - женщина, которая нашла свою нишу в мире перехвата пакетов в сети, стала мировым экспертом, и спустя более 20 лет она все еще лучшая в своем деле.

Подробнее о Лоре Чаппелл

Подробнее о Лоре Чаппелл вы можете найти на этих ресурсах:

- Университет Чаппелл: https://www.chappellu.com/
- Профиль Лоры Чаппелл в LinkedIn: https://www.linkedin.com/in/chappelllaura
- Твиттер Лоры Чаппелл: https://twitter.com/LauraChappell
- Блог «В лаборатории Лоры» (старый материал, но, тем не менее, важный): http://laurachappell.blogspot.com/

Глава 35. Взлом IoT

Сегодня мир компьютеров - это не только персональные компьютеры. Это автомобили, дома, телевизоры, холодильники, тостеры, очки, браслеты, кроссовки, приборы освещения, радионяни, медицинские приборы, и практически любой другой предмет, который по мнению продавца будет более востребован, если в нем будет компьютер или сенсор. Как правило, эти вещи подключены к интернету, и имеют свой IP-адрес (Internet Protocol address). Все они относятся к интернету вещей (Internet of Things, IoT). К сожалению, многие, если не большинство из них, очень небезопасны, и могут быть взломаны.

Как Хакеры Взламывают IoT?

Также, как и обычные компьютеры, используя одну или несколько уязвимостей в уровнях модели OSI (Open Systems Interconnection) (Физический, Канальный, Сетевой, Транспортный, Сеансовый, Представительский и Прикладной). Единственная разница в том, что IoT-устройство может не использовать традиционное железо или известную операционную систему (или даже не использовать никакую операционную систему). Хакеры должны узнать как можно больше об этом устройстве, исследовать компоненты и принцип работы, и найти уязвимости.

Например, предположим, что хакер хочет взломать IoT-тостер. Первый пункт на повестке дня - купить такой тостер и изучить всю документацию. Затем нужно выяснить, как это устройство подключается к сети и какие пакеты отправляет. Для этого нужно включить устройство и использовать сниффер. Можно получить невероятное количество информации об устройстве, "прослушивая", что оно делает или пытается сделать, когда начинает работать. Хакер может провести сканирование на наличие портов прослушивания, и вычислить используемые сервисы и операционную систему. При наличии консоли администратора, хакер попробует к ней подключиться. Он попытается выяснить, на каком языке написано ПО этого устройства и попробует найти программный интерфейс приложения (application programming interface, API).

Также для взлома IoT-устройств часто используется физический взлом. Хакеры разбирают устройство и изучают его компоненты, обращая внимание на сам чип и его маркировку. Большинство устройств использует распространенные чипы, о которых есть немало информации. Иногда

уязвимости чипа хорошо известны, и присутствуют на многих устройствах. Хакеры, специализирующиеся на железе, припаивают дополнительные контакты на чип, и даже делают собственные чипы, чтобы обойти аутентификацию и получить доступ к управлению устройством. Особое внимание они уделяют поиску входных и выходных портов. Им это необходимо для того, чтобы определить можно ли подключить к устройству свой отладчик (debugger).

Чтобы узнать, какая информация передается, а также изменить передаваемые данные и изучить последствия, хакеры используют MitM-атаки (man-in-the-middle). Часто они делятся полученной информацией на форумах, посвященных IoT, или даже на форумах конкретных IoT-устройств. Они даже создают виртуальные сообщества, посвященные определенному устройству, объединяя опыт различных участников сообщества.

Вот несколько примеров общедоступных описаний взлома IoT-устройств, которые интересно почитать:

- https://blog.avast.com/2015/11/11/the-anatomy-of-an-iot-hack/
- https://www.rapid7.com/docs/Hacking-IoT-A-Case-Study-on-Baby-Monitor-Exposures-and-Vulnerabilities.pdf
- https://securelist.com/analysis/publications/66207/iot-how-i-hacked-my-home/
- http://resources.infosecinstitute.com/hardware-hacking-iot-devices-offensive-iot-exploitation/

В целом, если вы можете провести пентест обычного компьютера, то можно провести пентест и IoT-устройств, разве что IoT-устройства требуют больше креатива и исследований, особенно, если вам незнакома их операционная система или чипы. Однако, помимо того, что их можно взломать, сделать это намного легче, потому что многие производители IoT-устройств не осознают риск и не уделяют защите достаточного внимания, по крайней мере сейчас.

Защита IoT-устройств

Не то, чтобы над улучшением защиты IoT-устройств не работают. Многие производители считают, что уделяют ей достаточно внимания. Десятки независимых групп, таких как IoT Village (https://www.iotvillage.org/) работают над тем, чтобы помочь производителям повысить безопасность их устройств. К сожалению, хакерские группы, такие как San Francisco IOT Hacking Meetup (https://www.meetup.com/San-Francisco-IOT-hacking-Meetup/) не менее активны и их работа более успешна. Когда производитель IoT-устройства говорит, что

его продукт хорошо защищен, он скорее всего ошибается. Как правило, сильно ошибается.

Так что же может сделать производитель IoT-устройств, чтобы обезопасить свой продукт? Ну, отнестись к безопасности также, как относятся к безопасности обычных компьютеров. С самого начала проводить моделирование угроз, и обеспечить жизненный цикл безопасной разработки (security design lifecycle, SDL) с самого начала до окончания поддержки продукта. Убедиться, что устройство использует самую последнюю версию ПО с самыми новыми патчами, и обеспечить автообновление устройства. Убрать все ненужное ПО, сервисы и сценарии. Закрыть все ненужные порты. Использовать надежное шифрование. Обеспечить конфиденциальность клиента. Не собирать ненужную информацию. Безопасно хранить нужную информацию о клиентах. Использовать надежные способы аутентификации, и проводить множество пентестов во время разработки и бета-тестирования продукта. Предлагать награду за обнаружение багов. Не наказывать хакеров, сообщивших о багах. По сути, взять все уроки информационной безопасности, полученные из мира компьютеров за несколько десятилетий, и применить их к IoT-устройствам.

К сожалению, большинство производителей не делают этого, и мы, судя по всему, обречены на слабую защиту IoT-устройств в ближайшие несколько десятилетий.

В следующей главе мы поговорим о Докторе Чарли Миллере, который считается одним из лучших хакеров автомобилей.

Глава 36. Доктор Чарли Миллер

Большинство людей, знакомых с именем Доктора Чарли Миллера и его работой знают его, как участника хакерского дуэта, способного сделать из вашего автомобиля игрушку с дистанционным управлением. Если вы видели новости последних лет о хакерах, способных дистанционно отдать команду автомобилю марки Jeep или другому, внезапно ускориться или даже съехать с дороги, то все они были связаны с Доктором Миллером. Журналист издания *Wired* описал свой опыт работы с Доктором Миллером и его партнером Крисом Валасеком.

Миллер и Валасек написали подробную работу под названием "Adventures in Automotive Networks and Control Units" ("Приключения в автомобильных сетях и блоках управления") (http://illmatics.com/car_hacking.pdf), в которой описали, какими компонентами автомобиля, критическими и не критическими, можно управлять, включая систему экстренного торможения, кондиционер, световую индикацию, коробку передач, системы мультимедиа, тормоза и даже рулевое управление. Многим из нас, этот документ дал возможность понять, как работает и взаимодействует сеть автомобильных компьютерных систем. В последующих версиях документа они выяснили, как можно делать это удаленно. Это была нирвана для хакеров автомобилей! Авторы даже выпустили собственные инструменты, облегчающие получение контроля над системами автомобиля.

Сама идея удаленного взлома автомобиля не была шокирующей, однако, после просмотра видео, где два парня взламывают автомобиль находясь от него на расстоянии 15 километров, угроза стала более реальной и вышла из разряда гипотетических. Доктору Миллеру не понадобилось активно продвигать идею, что в плохих руках такие технологии станут причиной аварий и смертей. До того, как Доктор Миллер начал постоянно публиковать свои открытия, производители не сильно занимались безопасностью автомобильных компьютерных систем (Неизвестность таких проблем была лучшей защитой). Исследования и приключения Миллера и Валасека все изменили. Производители стали принимать во внимание все негативные отзывы в СМИ и внимательнее относится к безопасности автомобильных компьютерных систем. Были даже слухи, что крупные автомобильные компании подавали в суд на тестировщиков. Они старались сорвать дополнительные расследования и новые открытия.

Когда я брал интервью у Доктора Миллера, он заверил меня, что на него и других хакеров никогда не подавали в суд, и даже не угрожали судом: "Подать в суд можно на каждого, но мы действовали профессионально. Это

поддерживает нашу репутацию и репутацию производителей. Они просили нас не раскрывать определенных подробностей в одной из наших предстоящих презентаций, но мы их все равно раскрыли, и никто не подал на нас в суд". Не то, чтобы автомобильным компаниям нравится то, чем он занимается. Несмотря на то, что Доктор Миллер опубликовал лучшие исследования по взлому автомобильных компьютерных систем, автопроизводители ни разу не отправляли ему личных или каких-то других приглашений, чтобы выступить с докладом о своих открытиях. А когда, на одной конференции, он попросил их о большей прозрачности в будущем, чтобы автомобильные хакеры могли обнаружить и искоренить больше багов, в ответ последовало громкое, звучное "Нет". По причинам, которые, к сожалению, склонны снова и снова повторяться в разных индустриях, компании, которые могли бы извлечь наибольшую пользу из исследований хакеров, считают последних лишь раздражающим фактором, а возможно даже и врагом. К счастью, времена изменились, и сейчас Доктор Миллер работает в Uber - некоторые полагают, что он обеспечивает безопасность их будущих беспилотных автомобилей.

Впервые, я встретил Доктора Миллера около десяти лет назад, когда он пытался стать высокооплачиваемым тестировщиком. Он получил степень бакалавра по математике в Северо-Восточном университете штата Миссури (Northeast Missouri State University) (теперь это Государственный университет Трумана, Truman State University), и степень доктора математических наук - в Университете Нотр-Дам. Хотя его устраивает, когда его называют доктором, Миллера часто можно встретить валяющим дурака в общественных местах, когда там много людей, в очках, как у Элтона Джона, старающимся развеселить друзей. Если вы представляете себе серьезного, профессионального автомобильного хакера, доктора наук, то Чарли Миллер не соответствует этому представлению.

До своей нынешней работы, он провел пять лет в Агентстве национальной безопасности (АНБ), три года работал на Твиттер, а остальное время был консультантом и работал в других компаниях. Благодаря своему прошлому и любви к математике Доктор Миллер заинтересовался криптографией, а затем и работой в АНБ. Для тех, кто не знает, АНБ (https://www.nsa.gov/) - передовое агентство по шифрованию/расшифровке в США, если не во всем мире. В стенах АНБ немало отличных специалистов по криптографии, одним из которых является Доктор Миллер.

Я спросил Доктора Миллера, как он стал специалистом в области информационной безопасности и профессиональным автомобильным хакером, и вот, что он ответил: "До работы в АНБ, я никогда не думал, что у меня получится (стать экспертом в области информационной безопасности). АНБ наняли меня в качестве специалиста по криптографии, и я подумал, что с этим и будет связана моя работа. В АНБ нужно каждые полгода менять офис (то есть, работать в другом подразделении), чтобы получить более широкое

представление о различных технологиях, которые интересуют АНБ. Нужно изучать различные темы, но я, так сказать, обманул их, и сделал так, чтобы меня готовили только как специалиста по информационной безопасности, и, в основном, вне сферы криптографии. Другие темы информационной безопасности были гораздо интереснее, чем криптография. Я сделал так, чтобы мои руководители думали, что каждый офис, в котором я находился, специализировался на совершенно другом направлении, но на самом деле, эти подразделения специализировались на нескольких, более узких темах информационной безопасности. Через три года, я узнал много классных вещей о безопасности данных. Мне посчастливилось оказаться в организации, где я должен был учиться и получал за это деньги.

Я спросил Доктора Миллера, как он начал взламывать автомобильные компьютерные системы. Он сказал: "Долгое время я взламывал компьютеры и телефоны. Но демонстрация взлома компьютера или телефона обычным людям не приносила ожидаемого понимания или восхищения. Но люди прекрасно понимают, к чему может привести самопроизвольный поворот руля или срабатывание тормозов. Это был хак, который не нужно было продвигать или продавать. Он продвигал себя сам и был доступен обычным людям. Мы не были первыми, кто взломал автомобильные компьютерные системы. До нас это сделали другие. Мы основали свою работу на их открытии, и хотели узнать, как далеко можно зайти".

С самого начала Доктор Миллер сделал себе имя, за считанные минуты одержав несколько побед в хакерских соревнованиях Pwn2Own. Соревнования Pwn2Own (https://en.wikipedia.org/wiki/Pwn2Own) проходят в Ванкувере, Канада. Хакер, взломавший операционную систему или ПО, в которых до этого не было обнаружено багов, получает денежные и другие призы. Каждый успешный взлом был новой "уязвимостью нулевого дня" – уязвимость о которой знают хакеры, но о которой неизвестно производителю.

В течение нескольких лет, главным событием соревнований Pwn2Own было появление Доктора Миллера, который использовал свои эксплойты с помощью которых он за несколько минут взламывал систему и забирал один или все главные призы. Он делал это столько раз, что, в конце концов, это соревнование приобрело славу места, где любая программа взламывается за несколько минут, после того, как Доктор Миллер или один из его конкурентов садится за компьютер. Несколько лет имя Доктора Миллера соотносилось именно с победой на этих соревнованиях, а не со взломом автомобильных компьютерных систем. Из-за того, что он успешно взламывал самые популярные операционные системы, браузеры и устройства, люди стали внимательнее к нему прислушиваться, когда он заговорил о взломе автомобильных компьютерных систем. Репутация опережала его. Мы знали, что он знает, о чем говорит, и, что он, скорее всего, добьется успеха.

Секрет успеха Доктора Миллера заключался в том, что для быстрого взлома он использовал фаззинг. Существует немало способов обнаружить ошибки в программе. Можно протестировать ее, проверяя все возможные комбинации и изменяя значения вручную. Можно провести статический анализ кода, используя программу проверки исходного кода (или проверив его самостоятельно), которая ищет определенные ошибки в написании ПО. Или можно случайно наткнуться на баг, просто используя программу. Десятилетиями эти три традиционных метода использовались для обнаружения самых серьезных багов.

В конце 1990-ых фаззинг стал инструментом для обнаружения невероятного количества багов, и любой разработчик ПО рискует выпустить свой продукт с огромным количеством уязвимостей нулевого дня, если он не проводит тестирование с помощью фаззинга. Для такого тестирования применяется программа (фаззер), которая автоматически вводит всевозможные значения, как правило, неожиданные для программиста или языка программирования (например, слишком длинные, содержащие случайные управляющие символы, "зарезервированные слова" и так далее) в рабочую версию программы, чтобы вызвать ошибки. Затем каждая обнаруженная ошибка проверяется либо программой-фаззером, либо вручную, чтобы узнать, можно ли использовать эту ошибку для взлома программы или операционной системы, на которой она работает.

Вот как Доктор Миллер описывает свои успехи, связанные с использованием фаззеров: "Я узнал о фаззинге в АНБ. Мне понравилась эта техника, потому что с ее помощью можно быстро обнаружить баги, и ее действительно легко использовать. Я запускаю фаззер, иду смотреть телевизор, затем иду спать, просыпаюсь и смотрю, что удалось обнаружить. Где-то в 2010-ом на конференции Blackhat (http://blackhat.com/), я использовал на сцене фаззинг в реальном времени для обнаружения багов, соревнуясь с другими ребятами. Они использовали программу статического анализа, а у меня был фаззер. Мне понадобилось несколько минут, чтобы настроить его, но затем, я буквально закинул ноги на сцену и, спустя час, победил".

ПРИМЕЧАНИЕ Если вас интересует фаззинг, существует множество коммерческих и бесплатных продуктов. Microsoft даже предлагает для этого достойное бесплатное решение: https://www.microsoft.com/en-us/springfield/.

Я спросил Доктора Миллера, почему в самом начале он больше всего фокусировался на взломе продуктов Apple. Он сказал: "В то время, в коде продуктов Apple не было надежного уровня защиты информации, особенно защиты памяти. И они не проводили фаззинг-тестирование. Я сделал это за них, и нашел множество багов, которые можно было использовать на Pwn2Own и других соревнованиях. В Microsoft и Microsoft Windows проводили такое

тестирование, в их программах есть встроенная защита памяти. У меня не было цели взломать Apple, чтобы что-то доказать. Просто в их продуктах было легче обнаружить баги, а мне не нужны дополнительные сложности".

В 2007-ом он стал первым известным человеком, который удаленно взломал iPhone, а в 2008-ом, в день, когда появился первый телефон на Android, он удаленно взломал и его. Позже в 2008-ом, Доктор Миллер обнаружил уязвимость нулевого дня в браузере Safari на MacBook Air, и выиграл $10 000. В 2009 и 2010 годах он снова взломал браузер Safari, и продолжил взламывать мобильные телефоны Apple. В 2011-ом, он обнаружил дыры в безопасности iOS на iPad и iPhone. Он наглядно показал, как через проверенное приложение из магазина Apple можно красть информацию, то есть взламывать владельцев их устройств. Он создал демонстрационную программу, которую разместил в App Store.

В этот момент поиски багов Доктора Миллера вызвали гнев Apple. Они обвинили его в нарушении условий соглашения с разработчиком (которые он, технически, не нарушал) и отобрали у него права на разработку и публикацию приложений в их магазине. Вот, как он описал эту ситуацию: "Они сказали, что забирают у меня developer ID (учетная запись разработчика ПО) на год. После того, как я снова обратился за его восстановлением, мне отказали. На данный момент у меня все еще нет developer ID (учетная запись разработчика ПО)". Большинство из тех, кто наблюдал за ситуацией, думали, что Apple будет учиться на своих ошибках, и предложит Доктору Миллеру оплату за его поиски багов или наймет его на работу.

Когда я впервые встретил Доктора Миллера, он отчаянно пытался найти высокооплачиваемую работу тестировщика. В то время лишь немногие зарабатывали на поисках багов. Большинство, как и Доктор Миллер, вообще ничего не получали. В то время у разработчиков было очень мало программ "По вознаграждению за обнаружение багов", тогда как сегодня, такие программы существуют повсеместно. На самом деле, большие суммы за обнаружение новых уязвимостей нулевого дня получали только киберпреступники, которым платили плохие парни и преступные организации. Время от времени, "белые шляпы" могли продавать баги официальным компаниям, которые впоследствии перепродавали их по самой высокой цене разработчикам, чтобы те смогли изучить и исправить эти баги. Так происходит и сейчас.

Но Доктор Миллер хотел работать в Apple, Microsoft или другой компании, которая оценила бы его энтузиазм и знания. Долгое время этого не происходило, по крайней мере, так, как он надеялся. Но, в конечном счете, его стремление привело его к высоким постам в Twitter и Uber. Вместе с этим, он выдвинул на первый план идею, что те, кто профессионально занимается поиском багов, должны получать оплату за свои усилия. Он не был главным ее сторонником, но много говорил об этом. Он даже начал кампанию под

названием “No More Free Bugs” (“Больше никаких бесплатных багов”). Сегодня, практически у всех крупных разработчиков ПО есть программа денежного вознаграждения за обнаружение багов, и хорошие охотники за багами могут получить официальную, высокооплачиваемую работу.

Я спросил Доктора Миллера, что он чувствовал в те дни, когда был вынужден работать консультантом, вместо того, что найти работу, соответствующую его знаниям и таланту. Он сказал: “В итоге, я стал работать выездным консультантом, и это неплохая должность для начала карьеры. Можно увидеть различные компании, их проблемы и атмосферу. Всего один раз мне заплатили за баг, который я обнаружил вне соревнования Pwn2Own, в 2007-ом. Я быстро понял, что выступать на конференциях мне нравится даже больше, чем получать оплату. Для меня важнее поговорить, поделиться своими знаниями, чем получать деньги, но при этом молчать”.

Те, кто был на его презентациях и конференциях знают, что Доктор Миллер любит веселиться, развлекать и учить аудиторию. Очевидно, что его интерес вызван не только весельем и деньгами, но и любопытством. Как только он что-то освоил, он переходит в другую область, к следующей цели. Он сказал мне: “Как только я нахожу в программе пять багов, она становится уже не такой интересной, и я двигаюсь дальше”. В то же время, он обнаружил уязвимости безопасности в других областях, например в NFC (Near Field Communication). Он также опубликовал три книги (https://www.amazon.com/Charlie-Miller/e/B0085NZ1PS/), в которых описан взлом систем Mac, iOS и фаззинг-тестирование.

Последний мой вопрос Доктору Миллеру звучал так: Считает ли он, что в ближайшее время автомобильные компьютерные системы будут достаточно безопасны? Он ответил: “Автомобили ничем не отличаются от компьютеров, а мы все еще не знаем, как создать идеальную защиту для компьютеров. Взлом автомобильных компьютерных систем похож на взлом сетей, так как в этих системах используется множество блоков управления. Проблема автомобилей в том, что можно нанести физический вред. Это поднимает ставки. Возможно, я не смогу остановить взлом компьютерной системы автомобиля, но есть немало способов, которыми я могу смягчить последствия самых страшных атак. Возможно, злоумышленники смогут “поиграться” с системой мультимедиа, но, если мы все сделаем правильно, то они не смогут получить доступ к тормозной и другим критически важным системам”.

Являясь бывшим сотрудником АНБ, он не рассказал мне, над чем именно он работает в Uber, но можно догадаться, что Uber и их пассажиры останутся в выигрыше.

Подробнее о Чарли Миллере

Подробнее о Чарли Миллере вы можете найти на этих ресурсах:

- Твиттер Чарли Миллера: https://twitter.com/0xcharlie
- Книги Чарли Миллера: https://www.amazon.com/Charlie-Miller/e/B0085NZ1PS
- Публикация "Adventures in Automotive Networks and Control Units": http://illmatics.com/car_hacking.pdf
- Публикация "Car Hacking: For Poories": http://illmatics.com/car_hacking_poories.pdf
- Публикация "A Survey of Remote Automotive Attack Surfaces": http://illmatics.com/remote%20attack%20surfaces.pdf
- Публикация "Remote Exploitation of an Unaltered Passenger Vehicle": http://illmatics.com/Remote%20Car%20Hacking.pdf
- Публикация "CAN Message Injection": http://illmatics.com/can%20message%20injection.pdf

Глава 37. Политики и Стратегии

Я был одним из тех, кто ненавидит политики и процедуры. Я не видел смысла в оформлении документации. Это только замедляет работу. Тогда я думал именно так.

После десятилетий упорной работы специалистом по информационной безопасности, я наконец понял, что без соответствующих основ и порядка действий ничего не получится. Кто угодно может защитить несколько компьютеров и устройств. Меня не взламывали почти два десятилетия. Но без "правильной" документации невозможно защитить компьютеры целой компании. В итоге я осознал необходимость стандартов, политик, процедур, основ, и начал ценить труд тех, кто пытается правильно их применить. Это настоящие "закулисные" герои, без которых мы не смогли бы сделать компьютеры значительно безопаснее.

В этой главе я разберу документы, которые представляют из себя стандарты, политики, процедуры, фреймворки и законы.

ПРИМЕЧАНИЕ Реже используются термины "руководство" или "практики".

Стандарты

Стандарты - это описания минимального набора норм, правил, протоколов и требований. В мире информационной безопасности, стандарты зачастую представляют из себя утверждения, такие, как:

- Во время передачи и хранения, все критически важные данные будут зашифрованы
- Минимальный размер открытого ключа должен составлять 2048 бит для алгоритмов RSA и Диффи-Хеллмана, и 384 бита для ECC.
- Пароли должны состоять, как минимум, из двенадцати символов и содержать, по крайней мере, два неалфавитных символа.
- После трех неудачных попыток введения пароля в течение пяти минут, аккаунт должен быть заблокирован, пока его не проверит администратор.
- Все критические обновления безопасности должны быть установлены в течение пяти рабочих дней с момента их выпуска производителем.

- На всех компьютерах должен быть установлен персональный файрвол, в котором по умолчанию должно работать запрещающее правило.

Как правило, стандарт представлен в виде политик и поддерживается соответствующими процедурами.

В некоторых случаях стандарты становятся нормативами, законами или требованиями, которые должны применяться к любому устройству. В США, одним из самых распространенных стандартов, который должны соблюдать десятки миллионов компьютеров - это United States Government Configuration Baseline (USGCB, Конфигурации безопасности для организаций, связанных с правительством США) (https://usgcb.nist.gov/). Производители также могут разрабатывать свои стандарты, например, Microsoft's Security Compliance Manager (Менеджер настроек безопасности для продуктов Microsoft) (https://technet.microsoft.com/en-us/library/cc677002.aspx). Иногда стандарты получают такое доверие и уважение, что становятся национальными или мировыми. Отличным примером служит практически каждый стандарт разработанный Национальным институтом стандартов и технологий (National Institute of Standards and Technology, NIST) (https://www.nist.gov/). А многие компании тратят огромные суммы и ресурсы, чтобы пройти сертификацию по стандартам ISO/IEC 27001 (http://www.iso.org/iso/home/standards/managementstandards/iso27001.htm).

Политики

Политики - задокументированные принципы, определяющие принятие решений для достижения желаемого результата. Зачастую, это документы, без которых применить соответствующие принципы было бы намного сложнее. Например, "Сотрудники не должны использовать один и тот же пароль для разных сетей". Хотя это не дает компаниям гарантии, что такого никогда не произойдет, наличие документа, о котором знают сотрудники, значительно снижает шансы нарушений. Кроме того, если о нарушении станет известно, то будет проще применить соответствующее наказание.

Процедуры (Порядок Действий)

Порядок действий - задокументированная последовательность шагов при работе и установке оборудования, направленная на поддержку стандартов и политик. Порядок действий обеспечивает их надлежащее и своевременное применение. Порядок действий может быть изменен, независимо от стандартов и политик, например, новая программа может потребовать другой порядок действий.

Фреймворки

Создание стандартов и политик для всего спектра информационной безопасности с нуля может быть очень сложной задачей. В этом могут помочь общие принципы, демонстрирующие наиболее распространенные стандарты, политики, форматы и содержащие обширный набор соответствующих тем. Отличный пример общих принципов кибербезопасности - это NIST's Cybersecurity Framework (https://www.nist.gov/cyberframework).

Регулирующие Законы

Стандарты и политики могут быть законодательно закреплены. Например компании, которые хотят обрабатывать большое количество наиболее распространенных кредитных карт, должны следовать стандартам Payment Card Industry Data Security Standard (стандарт безопасности данных индустрии платёжных карт, разработанный Советом по стандартам безопасности индустрии платежных карт) (https://www.pcisecuritystandards.org/). Отказ от следования стандартам PCI DSS может привести к временному отстранению от обработки данных платежных карт или даже наказанию на уровне закона. В США, организации, занимающиеся здравоохранением, должны следовать закону "О перемещаемости и подотчетности страхования здоровья" (Health Insurance Portability and Accountability Act, HIPAA). Любая компания, чьи бумаги торгуются на биржах США, должны следовать требованиям закона Сарбейнза-Оксли (Sarbanes-Oxley Act), и так далее.

Проблемы Компаний, Работающих на Мировых Рынках

В каждой стране, где работает международная компания есть свой набор стандартов и политик, часто конфликтующих со стандартами других стран. В некоторых странах высоко ценится неприкосновенность частной жизни, в то время, как в других, требования о ее неприкосновенности могут отсутствовать на уровне закона. Законы некоторых стран могут требовать, чтобы компьютерные системы, используемые в других странах, использовали более слабое шифрование (например, законы США об экспорте стандартов шифрования). Количество серьезных проблем компаний, работающих на международных рынках, постоянно увеличивается.

Системная Поддержка

Многим компаниям приходится работать с различными, иногда конфликтующими друг с другом требованиями. По этой причине была создана целая экосистема компаний и инструментов, помогающих следовать одному или нескольким стандартам или требованиям. Как правило, у компаний есть специальные команды, сотрудники, дорогое ПО, и директора, занимающиеся этой проблемой. Чтобы своевременно выполнять требования стандартов, нужны специальные сотрудники, целая IT-команда, и участие в общем деле каждого сотрудника. Соответствие требованиям - это целое направление бизнеса. Результатом неподчинения могут стать проблемы с законом, судебные процессы, а также наличие уязвимостей, которыми могут воспользоваться хакеры.

Если вы только что прочитали эту главу и жалеете о потерянных минутах жизни, потому что чуть не уснули, знайте, что когда-то я тоже считал все это пустой тратой времени. Десятилетиями я наблюдал за тем, как мои невероятно функциональные, точные рекомендации применяли неправильно или вовсе игнорировали. Это и привело меня к осознанию важности создания политик и документации. Без необходимой документации не может быть и речи о надежности информационной безопасности. Все просто.

В следующей главе мы поговорим о Цзин де Джон-Чен, работающей над улучшением международных стандартов безопасности и мирового киберправительства.

Глава 38. Профиль: Цзин де Джон-Чен

Как уже говорилось в предыдущей главе, без политик и стратегий нельзя достичь надежной информационной безопасности. Некоторые из "невидимых" героев в сфере безопасности информации занимаются созданием и продвижением корпоративных и международных стратегий информационной безопасности. Цзин де Джон-Чен, партнер и генеральный менеджер, представляющая отделы стратегии глобальной безопасности, корпоративных отношений, внешних связей и юридический отдел в Microsoft, посвятила свою профессиональную карьеру продвижению и улучшению мировых стандартов информационной безопасности и гармонизации политик кибербезопасности. Она также является вице-президентом Trusted Computing Group (TCG), некоммерческой, международной организации, разрабатывающей стандарты в индустрии информационной безопасности, чьей целью являются инновации технологий безопасности. Она также является членом консультативного комитета Executive Women Forum, организации, занимающейся продвижением женщин в профессиях, связанных с безопасностью, конфиденциальностью и управлением рисками. Кроме того, де Джон-Чен является советником проекта Digital Futures, созданного Международным научным центром имени Вудро Вильсона (Woodrow Wilson Center). В 2014-ом она получила премию "Women of Influence Award" от организации Executive Women Forum за профессиональный вклад в кибербезопасность. У нее есть степень магистра по управлению бизнесом и степень бакалавра по информатике.

Когда я впервые брал у нее интервью, я сразу обратил внимание, насколько содержательно и полно она отвечает на вопросы. Уже несколько десятилетий она успешно борется за улучшение мировых общественных политик и стандартов, а ее опыт и знания были неоднократно отмечены. Ее опыт уникален, как для женщины-специалиста, так и для профессионала из Азии, и она охотно это признает, поскольку является активным сторонником разнообразия в области информационной безопасности.

Я спросил, как она впервые попала в сферу информационной безопасности. Она ответила: "В 1992-ом я начала работать в Microsoft, а именно в отделе исследований и разработки, чтобы бороться с трудностями при создании азиатских версий Windows 3.1. В то время не было китайской версии Windows, а Китай активно продвигал экономические реформы и становился важной частью мировой экономики. Мы создали первые японские, корейские и китайские версии Windows 3.1, где поддерживался набор "двухбайтовых" символов. Чтобы соответствовать нашему видению демократизации

компьютеров, которое предполагало "компьютер в каждом доме и на каждом столе", мы должны были создавать наше ПО, с учетом пользователей по всему миру. Основываясь на тех трудностях, с которыми нам пришлось столкнуться при разработке Windows 3.1, мы поняли, что должны изменить подход к созданию программ. Мы разработали подход, предусматривающий использование одной кодовой базы, мы хотели использовать Юникод, и отделить ресурсы (языковые компоненты) от исходного кода.

К тому моменту, когда мы выпустили международную версию Windows 95, одновременно выпустив версии с поддержкой различных языков, мы сильно опережали многие компании, разрабатывающие ПО. Мы выпустили версию Windows 95 с поддержкой упрощенных китайских иероглифов через полгода после выхода американской версии. Это было достижением, учитывая усилия по локализации. Чтобы соответствовать национальному стандарту языка, мы добавили более 25 000 упрощенных и традиционных китайских иероглифов. Как вы знаете, Китай гордится тем, что является родиной книгопечатания, но до появления коммерческих операционных систем, таких, как Windows 95, выход в печать все еще требовал ручной работы. Мы работали с профессором Ванг Хуан, пионером Founder Group (китайской компании, специализирующейся на информационных технологиях), над созданием приложения для электронной публикации на базе Windows, которое моментально оказало влияние не только на Китай, но и китайские издательские сообщества, находящиеся за рубежом. После тысячелетий ручного труда это были первые шаги Китая на пути к электронной публикации. Это продемонстрировало ценность компьютеров, способных значительно увеличить производительность труда. Лично я была очень довольна результатом.

Затем в 1998-ом, примерно в начале революции в электронной коммерции, Microsoft заинтересовались интернет-пространством. Я стала работать в подразделении онлайн-услуг, но нельзя работать с интернет-сервисами и программами, не обращая внимания на безопасность. В течение нескольких лет, у нас были серьезные трудности, поскольку хакеры стали использовать вирусы и вредоносное ПО для того, чтобы навредить нам и нашим клиентам. Два примера - это Code Red и SQL Slammer. Все сотрудники Windows пытались выяснить, как можно создать более безопасное и надежное ПО. В то время, атаки 11 сентября показали, что индустрии, такие как финансовая, были лучше подготовлены к катастрофам и могли быстрее восстановиться. Уроки, полученные после проблемы Y2K (Проблема 2000 года) пошли на пользу этим компаниям. Я поняла, где проблемам безопасности уделяется наибольшее внимание и присоединилась к отделу расширенных политик и стратегии Microsoft (Microsoft's Advanced Policy and Strategy Division), под руководством Крейга Манди. Я стала работать в Trustworthy Computing Group, под руководством Скотта Чарни, и нашей целью были безопасность, конфиденциальность, надежность и корпоративная этика. Мне повезло

обучаться у двух очень опытных руководителей, как в области технологий, так и в области кибербезопасности.

Помню во время первых атак, серьезно пострадали такие рынки, как рынок Кореи и Японии, потому что они одними из первых перешли на наши технологии и начали работать в интернете. Влиянию этих атак подверглись миллионы пользователей. Правительства были обеспокоены. У Microsoft было совсем немного времени, чтобы отреагировать. Я полностью посвятила себя проблемам информационной безопасности и работе с правительством. Я начала заниматься пропагандой и искала способы помочь наладить партнерские отношения между государственным и частным секторами для минимизации рисков и комплексного решения вопросов безопасности. У нас была возможность делиться знаниями и разрабатывать решения для поддержки правительственных и корпоративных партнеров. Например, в различных странах, в управлении полиции использовались очень старые системы, и не было подразделений, занимающихся кибербезопасностью. Когда расследование киберпреступлений стало более приоритетной задачей, структурам правопорядкам понадобилось больше экспертов, способных реагировать на эти инциденты и проводить экспертный анализ. Microsoft выступили в поддержку этих усилий, обеспечивая необходимую техническую подготовку, в том числе, в таких регионах, как Юго-Восточная Азия.

У меня супердинамичная работа, и мне повезло сотрудничать с коллегами и единомышленниками, которые многому меня научили. Microsoft стали чемпионом в области технологий и стратегий кибербезопасности. Мы расширили границы своих взглядов, мы стали смотреть и внутрь, и наружу. Плюс мы стали работать с партнерами. Тогда сотрудничество конкурентов было редким явлением, но мы верили, что кибербезопасность важнее конкуренции. Мы делились способами защиты важной информации с поставщиками антивирусов, и разработали правительственную программу защиты (Government Security Program) для улучшения ситуации в области кибербезопасности, как в развивающихся, так и в развитых странах. В конце концов, в 2008-ом я стала работать над аппаратными решениями для обеспечения безопасности, и с тех пор продолжала деятельность в Trusted Computing Group, где мне довелось работать со многими талантливыми людьми".

Я поинтересовался, с какими проблемами ей приходится сталкиваться и какие проблемы ей приходится решать на посту вице-президента Trusted Computing Group (TCG). Она привела пример: "Вы знаете о чипе Trusted Platform Module (TPM), который помогает обеспечить безопасность компьютеров на аппаратном уровне. Версия TPM 1.2 работала отлично, но ей не хватало гибкости, чтобы "спрятать" алгоритмы шифрования при обнаружении уязвимости. В то же время, различные страны начали продвигать использование собственных алгоритмов в своих продуктах для обеспечения безопасности. В TPM 1.2 было

невозможно удовлетворить это требование, поскольку в этой версии поддерживался только определенный набор алгоритмов.

Появился риск конкуренции с правительствами на уровне стандартов, перед тем, как эта технология станет использоваться международно. Если страны пойдут по пути разработки несовместимых стандартов, то только из-за использования собственного алгоритма пострадает безопасность всех пользователей. С точки зрения внедрения этой технологии, это неизбежно привело бы к проблемам совместимости между чипами безопасности, основанными на международных стандартах, и теми, которые разработаны в соответствии со стандартами определенной страны. В TCG приняли решение разобраться с этой проблемой "подвижности шифрования", помимо других улучшений, которые были представлены в версии TPM 2.0. Благодаря усилиям многих экспертов по безопасности из разных стран, стандарт TPM 2.0 был принят, как ISO/IEC 11889:2015. Теперь это уникальный стандарт, который используется во всем мире. Это очень значимое событие, поскольку потребовалось согласие между многими странами, включая США, Китай, Россию, Канаду, Японию, Францию, Южную Африку, Малайзию и другие. Мы действительно достигли чего-то особенного. Новый стандарт предлагает гораздо более широкий уровень безопасности информации не только для пользователей PC, но также для облачных решений и IoT-устройств". Мне было очевидно, что работа де Джон-Чен по глобализации Windows 95 принесла плоды, когда она помогала разрабатывать мировой стандарт информационных технологий и экосистему.

Я спросил, что на ее взгляд является самым большим препятствием для значительного улучшения мировой информационной безопасности. Она ответила: "В разных странах разное мировоззрение, и это нужно учитывать, продвигая международные стандарты безопасности и наиболее эффективные подходы. Есть проблемы, связанные с политиками и технологиями. Разумеется, что технические специалисты хотят создать лучшую технологию, но это лишь часть проблемы. Существуют проблемы экосистемы и киберправительства. Каждая страна стремится защитить свой суверенитет в киберпространстве, пытаясь добиться в этой области максимально возможных результатов. Нельзя решать только технологические проблемы или оставить кибербезопасность политикам. Нужно найти наилучшее решение и баланс соответствия самым различным требованиям. И это превращается в очень сложную систему, которую должны учитывать высшее руководство и лидеры индустрии перед тем, как что-то делать. Политические вопросы учитывают: безопасность и конфиденциальность интернет-пользователей, защиту критической инфраструктуры, социальную и экономическую стабильность, а также международные связи и торговлю. Чем больше стран выпускают собственные нормы безопасности, тем выше цена организаций, занимающихся международной торговлей. Для того, чтобы соответствовать требованиям,

необходимо учитывать политические последствия, правовые риски, изменения проекта и изменения бизнес и операционной модели. Есть множество трудностей и возможностей, но нельзя решить крупные, общие проблемы информационной безопасности, без понимания внутреннего устройства страны и взаимосвязи различных элементов. Если все делать правильно, то возможно у нас получиться достичь равновесия, необходимого для улучшения кибербезопасности и защиты информационной инфраструктуры, и, при этом, обеспечить безопасность частных данных пользователей, честную конкуренцию, и при этом значительно снизить стоимость ведения бизнеса при международной торговле".

Я спросил о недостатке женщин в IT-индустрии. Де Джон-Чен ответила: "В целом, в IT-индустрии работает мало женщин, но их еще меньше в сфере информационной безопасности. Я работала с крупной интернет-компанией, где активно нанимали женщин, и видели в них потенциал. Даже несмотря на то, что пятьдесят четыре процента сотрудников составляли женщины, я этого не заметила, когда общалась с их командой по обеспечению безопасности. Там была только одна женщина, и она была не специалистом по безопасности, а координатором. В мире кибербезопасности нужно больше талантов, и мы должны найти способ привлечь и удержать женщин в IT-индустрии, и тем самым, обеспечить разнообразие специалистов в сфере информационной безопасности. Нам нужны все для достижения этой цели".

Подробнее о Цзин де Джон-Чен

Подробнее о Цзин де Джон-Чен вы можете найти на этих ресурсах:

- Блог Цзин де Джон-Чен в Microsoft: http://blogs.microsoft.com/microsoftsecure/author/jingdejongchen/
- Профиль Цзин де Джон-Чен в LinkedIn: https://www.linkedin.com/vsearch/p?rig=SEO_SN&firstName=Jing&lastName=Jong-Chen&trk=SEO_SN
- "Governments Recognize the Importance of TPM 2.0 through ISO Adoption" (Публикация в Microsoft Secure Blog): http://blogs.microsoft.com/microsoftsecure/2015/06/29/governments-recognize-theimportance-of-tpm-2-0-through-iso-adoption/
- "U.S.-China Cybersecurity Relations: Understanding China's Current Environment" (Статья в журнале *Georgetown Journal of International Affairs*): http://journal.georgetown.edu/u-s-china-cybersecurity-relationsunderstanding-chinas-current-environment/
- Spotlight on Cyber V: Data Sovereignty, Cybersecurity and Challenges for Globalization (Статья в журнале *Georgetown Journal of International Affairs*): http://journal.georgetown.edu/data-sovereignty-cybersecurity-andchallenges-for-globalization/

Глава 39. Моделирование Угроз

Моделирование угроз представляет собой изучение наиболее вероятных и значимых угроз в прогнозируемом варианте развития событий, с определением их потенциального урона за конкретный период времени, и поиском наиболее экономичных способов уменьшения их вреда, для обеспечения защиты от самых приоритетных угроз. Моделирование угроз применяется во всех индустриях, в том числе и в нашем случае, для определения способов защиты информации. Моделирование угроз применяется в security development lifecycle (SDL) при написании и проверке программ, а также во время их работы на компьютерах и в инфраструктуре. Именно моделирование угроз позволяет защитникам определять количество угроз, рисков и средств, необходимых для уменьшения негативных последствий, а также сравнить используемый план действий с реальными ситуациями.

Зачем Проводить Моделирование Угроз?

Моделирование угроз снижает риски. По крайней мере, оно позволяет одному или нескольким специалистам рассмотреть различные угрозы и риски в данном сценарии работы. Оно позволяет оценить последствия различных угроз, оценить и разработать средства предотвращения этих последствий, и, вероятно, такие средства будут эффективными и экономически выгодными. Мы совершенно точно знаем, что в долгосрочной перспективе, программы, при создании которых использовалось моделирование угроз, имеют меньше багов и уязвимостей. Если моделирование проводится впервые, то тестировщики могут обнаружить больше багов и уязвимостей, чем было обнаружено ранее, и в течение определенного периода, их количество может увеличиваться, но в конечном счете, новых багов и уязвимостей будет все меньше. В результате, на протяжении всего периода существования проекта или продукта, общее число багов и их негативных последствий должно быть меньше. А зачем еще проводить моделирование угроз?

Моделирование угроз учитывает, в том числе, и экономическую выгоду от внедрения средств предотвращения негативных последствий. Стоимость внедрения таких средств может быть настолько высокой (учитывая цену, затраченные ресурсы, возможные проблемы производительности, и так далее), что, несмотря на возможные риски, будет выгоднее их не использовать. Например, предположим, что компьютерные вирусы ежегодно наносят

компании урон в $100 000. Вряд ли эта компания захочет тратить больше, чем $100 000, чтобы остановить эти вирусы. Это очень простой, но наглядный пример того, что для компании будет выгоднее не тратиться на средства антивирусной защиты.

Используемые Модели Угроз

Моделей угроз существует не меньше, чем их видов. Как правило, названия моделей представляют из себя акронимы, такие как STRIDE, PASTA, VAST, TRIKE и OCTAVE. Есть множество программных инструментов, которые работают на основе собственных моделей, либо на основе уже существующих. У каждой модели есть сторонники и критики. Для разработчиков и поставщиков средств обеспечения безопасности информации намного важнее проводить моделирование угроз, используя любую модель, чем не проводить его вовсе, если они не могут определиться, какую модель выбрать. Моделирование угроз, в любом случае, приносит пользу.

Каждая модель пытается учитывать понимание того, чем, в совокупности, является рассматриваемый проект. Как правило, для этого используются методы мозгового штурма, построения диаграмм, а также подробное описание всех процессов работы. Затем рассматриваются все потенциальные угрозы для данного проекта, программы или сервиса. Оценивается их вероятность и потенциальный урон. В первую очередь рассматриваются угрозы и риски, которые могут нанести наибольший урон. Затем разрабатываются средства предотвращения негативных последствий, а также оценивается их эффективность и экономическая выгода по отношению к каждой конкретной угрозе.

Любая модель должна начинаться с понимания того, какой оставшийся (остаточный) риск желает получить или может себе позволить клиент, после принятия защитных мер. Например, моделирование угроз для наступательного или оборонительного вооружения начинается с понимания того, что остаточный риск должен быть минимальным. Одна компания может позволить себе максимально уменьшить остаточный риск, в то время, как ресурсы другой компании сильно ограничены, и она вынуждена согласится с принятием гораздо более серьезных рисков. Моделирование угроз помогает пользователям лучше подготовиться к работе, с учетом остаточного риска. С той же целью, некоторые модели уделяют внимание на "известным неизвестным" ("known unknowns") и "неизвестным неизвестным" ("unknown unknowns"), а также, напоминают пользователям, что невозможно рассмотреть и предотвратить все риски.

Каждая модель также должна учитывать разнообразие хакеров, которые могут ее атаковать. Существует огромное количество злоумышленников и у всех своя мотивация.

Правительственные Хакеры

В большинстве развитых стран есть команды из умных, способных и обеспеченных ресурсами хакеров, которые настроены патриотично, и работают либо в интересах правительства, либо в интересах армии. Они атакуют и взламывают стратегические объекты других стран. Неотъемлемый компонент в работе таких хакеров - это кибероружие. Кибероружие состоит из вредоносного ПО, и применяется профессиональными хакерами. Они стараются помешать противнику вести войну или построить надежную защиту. Отличный пример - червь Stuxnet, который уничтожил ядерную инфраструктуру целой страны. Прочие угрозы время от времени могут появляться и исчезать, но правительственные хакеры будут всегда.

Хакеры, Работающие в Интересах Конкурентов

Некоторые хакеры крадут секреты и интеллектуальную собственность различных компаний для последующей перепродажи другим компаниям. Хакеры, представляющие такую угрозу, могут работать на конкурентов, действуя либо в интересах определенного государства, либо в качестве фрилансера.

ПРИМЕЧАНИЕ Хакеры, работающие как на правительство, так и на конкурентную организацию совершают целевые кибератаки (Advanced Persistent Threats, APT, “развитая устойчивая угроза”). APT-атаки совершаются скоординированными усилиями профессионалов, которые остаются в системе противника в течение длительного периода. Как, правило, для них выделяются огромные ресурсы, и их, практически невозможно остановить.

Финансовые Преступления

Финансовые киберпреступления совершаются злоумышленниками, которые распространяют программы-вымогатели, используют DDoS-атаки, создают рекламное ПО, а также хакерами, заинтересованными в краже цифровой валюты, данных аутентификации и персональных данных. Деньги интересовали преступников задолго до появления компьютеров, но нынешнее состояние информационной безопасности позволяет злоумышленникам красть больше

денег, и, при этом, рисковать меньше, чем при совершении обычных преступлений, не связанных с компьютерами.

Хакеры-активисты

Люди, которые мотивированы политическими, моральными и психологическими идеями. Они часто склонны наносить вред (финансовый, репутационный, и так далее) компаниям и организациям, с которыми они не согласны. Одни из самых масштабных атак в истории, были совершены хакерами-активистами.

Геймеры

Компьютерные игры и геймеры - это один из главных движущих факторов, которые вынуждают создателей ПО и железа совершенствовать производительность и технологии. Сегодня люди платят не только за то, чтобы поиграть, но и за то, чтобы посмотреть, как играют другие. На киберспортивных соревнованиях собирается не меньше фанатов, чем раньше собиралось на концертах рок-звезд. Иногда кажется, что половина всей телевизионной рекламы, которую показывают во время трансляции популярных событий (таких, как чемпионат Super Bowl) - это реклама компьютерных игр. Сказать, что сегодня компьютерные игры приобрели большую популярность - все равно, что ничего не сказать. Некоторые хакеры считают своей целью исключительно взлом компьютерных игр. С помощью взлома игр они стараются повысить свой показатель побед (во всех смыслах), получить игровое преимущество и навредить игровым сервисам, которые их не устраивают.

Угроза Инсайда

Вопрос о том, насколько серьезную угрозу могут представлять собственные сотрудники, обсуждался всегда, но очевидно, что немалая часть всех атак совершается изнутри. Некоторые сотрудники крадут данные или прочую интеллектуальную собственность для последующей продажи конкурентам или для получения преимущества при устройстве на другую работу. Другие крадут деньги или информацию, например, данные кредитной карты клиента (для личного обогащения). Очень сложно обнаружить и помешать сотрудникам, которые совершают несанкционированные действия, особенно, когда они проводят транзакции, используя свои должностные полномочия. Индустрия информационной безопасности все еще испытывает трудности в борьбе с этой угрозой.

Обычные Хакеры-одиночки или Хакерские Группы

Давайте не будем забывать об обычных хакерах, которые взламывают, ради своих собственных целей, будь то финансовая выгода или просто, чтобы доказать, что они умеют взламывать. Больше десяти лет назад такие хакеры были доминирующим большинством. Тогда среди хакеров редко встречались профессиональные киберпреступники. В основном, они просто писали вирусы, которые высвечивали на компьютере забавные надписи или в определенный момент проигрывали “Yankee Doodle Dandy”. Некоторые вирусы наносили серьезный урон, например, Michelangelo, который форматировал жесткие диски. Но, как правило, это были просто проекты, целью которых было просто показать остальным, что автор достаточно умен и смог его создать. У этих хакеров не было цели нанести серьезный, масштабный урон.

Все разработчики и специалисты по информационной безопасности должны проводить моделирование угроз. Это значительно снижает риск и позволяет ранжировать угрозы, основываясь на их потенциальном вреде. Те, кто не проводит моделирование угроз, могут только догадываться какие средства защиты необходимо установить.

В следующей главе мы поговорим об Адаме Шостаке, уважаемом специалисте по моделированию угроз и авторе нескольких книг.

Глава 40. Профиль: Адам Шостак

Одна из моих первых встреч с Адамом Шостаком была в Microsoft, когда он продвигал новый способ решения проблемы. Конкретно в том случае, нужно было решить, как победить червя Conficker (https://en.wikipedia.org/wiki/Conficker). Conficker был очень неприятной вредоносной программой, которая впервые появилась в конце 2008-го. Она распространялась несколькими способами (то есть, через разные "векторы"), включая подбор слабых паролей передаваемых файлов, трюк с desktop.ini, уязвимости ПО, а также через USB-ключи, используя встроенную в Windows функцию автозапуска. Ежегодно Conficker заражал миллионы машин, и он не снижал «обороты». Производители защитного ПО могли легко его обнаружить, и Microsoft выпустили несколько статей о том, как остановить его распространение, однако червь все равно продолжал заражать компьютеры пользователей.

Чтобы детальнее разобраться в проблеме Шостак предложил использовать анализ данных. Он и Microsoft начали изучать, какие векторы атаки позволяли червю Conficker наиболее эффективно распространяться. Сначала мы предполагали, что большинство пользователей были заражены, потому что не установили патч, который был давно выпущен. И первое время, это действительно был один из самых популярных векторов. Но к тому моменту, спустя уже почти два года, Шостак обнаружил, что, в основном, заражение происходило через USB-ключи. Учитывая собранные данные, он предложил Microsoft отключить функцию автозапуска, что было очень серьезным решением. Это бы привело изменениям в работе Windows и, с этого момента, вынуждало всех пользователей, не только зараженных, совершать дополнительные действия для запуска программы на съемном носителе. Но у Шостака были данные. Они были той силой, которая позволяла применить такой подход, и в следующем патче, в нем Microsoft добавили обновление, которое отключало функцию автозапуска. И вот так просто Conficker умер. Ну, то есть, он не умер окончательно, но с того момента он перестал быть огромной проблемой. На самом деле, с того момента, распространение вредоносного ПО через USB-ключи перестало быть серьезной проблемой.

Подход Шостака и Microsoft, учитывающий использование данных для реакции на проблему оказал на меня сильное впечатление. Благодаря этому, я выпустилна мой взгляд, самую важную работу в своей карьере "Implementing a Data-Driven Computer Security Defense" (https://gallery.technet.microsoft.com/Fixing-the-1-Problem-in-2e58ac4a), которую,

впоследствии, стали рекомендовать к прочтению многие сообщества и светила индустрии.

Позже я прочитал книгу Шостака, которая называется *Threat Modeling: Designing for Security* (https://www.amazon.com/Threat-Modeling-Designing-Adam-Shostack/dp/1118809998), изданную Wiley. Было очевидно, что он действительно понимает, как нужно проводить моделирование угроз, а также ошибки других моделей и методов. Это все еще одна из первых книг, которые я рекомендую тем, кто интересуется моделированием угроз. Шостак был очень тесно связан с Microsoft, помогая с различными проектами, включая изменения в работе автозапуска, которые необходимо было провести для остановки червя Conficker. Помимо этого он также создал инструмент для моделирования угроз SDL Threat Modeling Tool (https://www.microsoft.com/en-us/sdl/adopt/threatmodeling.aspx). Плюс он является сооснователем Privacy Enhancing Technologies Symposium (Симпозиум по улучшению технологий защиты частных данных) и International Financial Cryptography Association (Международная ассоциация финансовой криптографии). Также он активно пишет, ведет блог и выступает на конференциях.

Я спросил, как он попал в сферу информационной безопасности. Он сказал: "Как специалист, я работал системным администратором в лаборатории медицинских исследований, и безопасность была частью моей работы. Это был 1993-ий и 1994-ый. Я начал читать некоторые мейл-листы, например, мейл-листы о первых файрволах и киберпанке. В этих мейл-листах разные интересные люди рассказывали об интересных вещах. Я начал участвовать в дискуссии и понял, что могу внести свой вклад. Моя следующая работа была более ориентирована на безопасность. Я стал консультантом в Бостоне. В то время интернет только начал набирать большую популярность. Так что знания о безопасности и возможность внести вклад в интернет-безопасность очень ценились. Кое-где я мог обнаружить уязвимости и это помогло заработать репутацию".

Я попросил его привести пример. Он ответил: "Я обнаружил уязвимость в брелке безопасности. Это был предшественник RSA Secure ID, позже RSA купили эту технологию. Уязвимость заключалась в том, что информация из предыдущего сообщения использовать для обеспеспечения безопасности следующего сообщения. Однако, в их алгоритме была уязвимость, которая связывала предыдущее сообщение с последующим, что делало ключ для этих сообщений более предсказуемым, и, следовательно, уязвимым".

Я спросил, как он начал работать с проектом CVE (Common Vulnerabilities and Exposures), базой данных общеизвестных уязвимостей информационной безопасности. Он пояснил: "Одним из клиентов, которых я консультировал, была компания Fidelity Investments. Они поручили мне обеспечить безопасность кода, тем же я занимался в Microsoft, спустя 15 лет. Я все еще активно пользовался мейл-листами и интернетом, делился знаниями и получал

обратную связь. Я всегда буду благодарен руководителям, которые позволяли мне это делать, потому что не все руководители или компании позволяют делиться такими знаниями. После Fidelity я стал работать в венчурной компании, которая владела частью организации, занимающейся разработкой сканера уязвимостей, и я подумал, что это будет интересно, поэтому перешел туда. Мы приложили все усилия, чтобы наш продукт мог обнаружить максимальное количество уязвимостей. Я работал над новой уязвимостью программы fingerd, и не знал, могут ли продукты наших конкурентов обнаружить эту уязвимость. В то время информации об уязвимостях было ничтожно мало, а поисковые системы работали отвратительно. Найти информацию было далеко не так просто, как сегодня. Мне стало интересно, как можно наладить контакт с другими специалистами, которые исследуют ПО, и узнать, какие уязвимости мы смогли обнаружить, а какие нет, и это привело меня к размышлениям о том, как контактировать с системными администраторами. Нам была нужна система, которая позволила бы объединить различных специалистов, чтобы они могли обсудить одну и ту же проблему на понятном всем языке. База данных CVE оказалась этой системой".

Я спросил Шостака о его самом влиятельном вкладе в моделирование угроз. Он ненадолго задумался, а затем ответил: "Я прислушивался к людям, когда они говорили, что что-то не работает. Некоторые учат других, как надо делать, чтобы работало, но я вижу, что такой подход не работает и что нужно менять саму систему. Например, если кто-то продолжает открывать зараженные электронные письма, даже, если им говорят, что этого делать нельзя. На мой взгляд это проблема системы, а не пользователя. Мы должны создавать системы, которые учитывают действия людей, потому что это не они делают что-то не так. Проблема в системах. Я читаю о системах безопасности в самолетах, потому что в сфере информационной безопасности мы не проводим достаточно тщательный анализ собственных ошибок. А в индустрии производства самолетов проводят. Даже если случается происшествие без последствий, то существует форма, которую может заполнить любой пилот, описав это происшествие, и отправить в соответствующую организацию. Эта организация собирает все формы и анализирует каждую из них. Они могут обнаружить одни и те же ошибки, даже если поначалу, причиной такого происшествия считался человеческий фактор. Организация может направить рекомендацию на радиозавод, и сообщить им, как можно решить проблему с радиосвязью, добавив лампочку, или сообщить определенному аэропорту (или нескольким аэропортам), как решить проблему с освещением ВПП. Это безупречный анализ основных причин. В сфере информационной безопасности не проводится достаточного анализа, поэтому мы повторяем одни и те же ошибки, снова и снова, и создание более совершенных систем занимает больше времени".

Я закончил наше интервью спросив его о том, что он может посоветовать молодым людям, которые интересуются информационной безопасностью. Он ответил: "Две вещи. Во-первых, я думаю, студенты могут получить преимущество, изучая гуманитарные науки (психологию, философию, и так далее). В самом начале карьеры, я изучал экологию. Я узнал, что проблемы окружающей среды являются следствием политических, правовых и экономических проблем, и если не решить эти проблемы, то не получится решить проблемы окружающей среды. То же самое и в информационной безопасности. Определенно, существуют технические проблемы, но, чтобы их решить, необходимо понимать политические, правовые и экономические проблемы. Это не проблема одного файрвола. Также, нужно научиться грамотно писать. Во-вторых, технические навыки не так важны, как правильное мышление. Технологические проблемы, с которыми я столкнулся, когда только начинал работать в этой области, не сравнимы с теми, которые существуют сегодня. Но мой подход остался прежним. Я изучаю большую проблему и задаю вопрос "почему что-то не работает?". Я подхожу к проблеме с точки зрения широкого вопроса и затем сужаю фокус, чтобы решить ее. Нельзя моментально решить серьезную проблему. Читатели должны уметь выбирать действительно важные проблемы, те, которые имеют значение, они должны уметь задавать правильные вопросы, а затем искать средства для решения этих проблем".

Подробнее об Адаме Шостаке

Подробнее об Адаме Шостаке вы можете найти на этих ресурсах:

- Книга *Threat Modeling: Designing for Security*: https://www.amazon.com/Threat-Modeling-Designing-Adam-Shostack/dp/1118809998
- Книга *The New School of Information Security* (в соавторстве с Эндрю Стюартом): https://www.amazon.com/New-School-Information-Security/dp/0321814908
- Веб-сайт Адама Шостака: https://adam.shostack.org/
- Твиттер Адама Шостака: http://twitter.com/adamshostack
- Профиль Адама Шостака в LinkedIn: http://www.linkedin.com/in/shostack/

Глава 41. Образование в сфере информационной безопасности

Практически всех людей, представленных в этой книге, объединяет убеждение в необходимости более качественной подготовки в сфере информационной безопасности. Никто не думает, что в ближайшее время появится идеальное технологическое решение, которое позволит людям не волноваться об угрозах информационной безопасности и о том, как с ними справиться. Некоторые "эксперты" по информационной безопасности заявляют, что обучение конечных пользователей - это пустая трата времени, но большинство настоящих профессионалов знают, что подготовка конечных пользователей и сотрудников приносит только пользу.

Мой нынешний наниматель, компания Microsoft, заставляет всех сотрудников проходить ежегодную подготовку по информационной безопасности на различные темы. Однажды, после многочисленных попыток взломать наших сотрудников с помощью фишинговых электронных писем, в обязательном к просмотру видео был уважаемый сотрудник Microsoft, который стал жертвой фишинга. Его уважали коллеги, и он работал в сфере, которая требовала больших знаний об информационной безопасности. Вкратце, он должен был быть последним, кто может стать жертвой социальной инженерии через фишинговые электронные письма, но это произошло именно с ним. Он поделился своим опытом, рассказал, как стал жертвой продуманного целевого фишинга. Было удивительно смотреть, как один из наших технологических лидеров рассказывал о том, что он не совершенен, что он может совершать ошибки, и том, как произошла эта ошибка. Он также рассказал, что несмотря на то, что ему было неловко за эту ошибку, ему не было слишком стыдно, и он позвонил в отдел IT-безопасности и сообщил об этом инциденте. Это обучающее видео было невероятно хорошо воспринято и позволило значительно снизить количество успешных фишинг-атак. Такая подготовка была настолько успешной, что команды IT-безопасности Microsoft весь год были завалены обращениями сотрудников, которые спрашивали, являются ли настоящие письма, которые выглядят подозрительно, фишингом. Некоторые даже говорили, что такое обучение было слишком успешным.

В предыдущие годы в образовательных видео рассказывали о том, как не выдать свой пароль, а также о необходимости убедиться, что никто не зашел за вами без соответствующего бейджа. Образование помогает значительно снизить влияние угроз информационной безопасности.

Существует множество вариантов и подходов подготовки в сфере информационной безопасности. В следующих разделах описаны некоторые темы, которые могут быть полезны тем, кто интересуется подготовкой в сфере информационной безопасности.

Подготовка Конечных Пользователей/Повышение Осведомленности

Такой вид подготовки, как правило, учит пользователей более безопасной работе со своими компьютерами и устройствами. Он раскрывает основные виды взлома, которым они могут быть подвержены, а также дает знания о том, как обнаружить, предотвратить и сообщить об атаке. Такое обучение должны пройти все, неважно,
пользуетесь ли вы компьютером дома, в школе или в офисе. Его нужно проходить, как минимум, раз в год, и в нем должны быть описаны недавние и наиболее вероятные угрозы. Как правило, такая подготовка занимает от 15 минут до нескольких часов каждый год.

Общая Подготовка по IT-безопасности

Эта подготовка необходима для IT-специалистов и сотрудников сферы информационной безопасности. Такая подготовка должна включать общие сведения обо всех видах взлома и вредоносного ПО, и более детально описывать основные и наиболее вероятные угрозы. Как правило, такая подготовка длится несколько дней или недель и может проводится повторно для достижения наилучшего эффекта.

Мероприятия по Реагированию

Сотрудники сферы информационной безопасности и, в особенности, участники команд по реагированию на инциденты должны быть обучены, как правильно реагировать и вести работу при возникновении экстренных ситуаций, связанных с информационной безопасностью. Такую подготовку должен проходить весь соответствующий персонал. Как правило, она длится несколько дней, и при необходимости должна проводится повторно.

Специальная Подготовка по ОС или Приложению

Многие производители популярных ОС или приложений предлагают общую и специальные программы по работе со своим продуктом. Специальная

подготовка производителя может дополнить общие знания по безопасности, и, в случае прохождения теста, как части сертификации, может подтвердить знания определенного продукта.

Технические Навыки

Многие организации, проводящие обучение и сертификацию, предлагают техническую подготовку по безопасности. Она включает изучение навыков использования определенных видов средств обеспечения безопасности, таких, как файрволы, системы обнаружения вторжения, анализ вредоносного ПО, криптография, выпуск патчей, создание резервных копий и так далее.

Сертификаты

Существуют десятки сертификатов по информационной безопасности. Изучение и/или прохождение теста для получения каждой сертификации повышает общие знания кандидата. Не бывает правильных или неправильных сертификатов. Однако, определенно, существуют сертификаты, определяющие соответствие уровня знаний, к которым в индустрии относятся с большим уважением. В целом, сертификат любой, из представленных ниже компаний, предоставляет широкие возможности (порядок не имеет значения):

- Международный консорциум по сертификации в области безопасности информационных систем (International Information Systems Security Certifications Consortium, ISC^2) (https://www.isc2.org/)
- Международный совет консультантов по электронной коммерции (International Council of Electronic Commerce Consultants, EC-Council) (https://www.eccouncil.org/)
- Институт системного администрирования, сетей и безопасности (SysAdmin, Networking, and Security Institute, SANS) (http://www.sans.org)
- Ассоциация индустрии информационных технологий (Computing Technology Industry Association, CompTIA) (https://certification.comptia.org/)
- Ассоциация контроля и проверки информационных систем (Information Systems Audit and Control Association, ISACA) (https://www.isaca.org)

Microsoft, Cisco и RedHat также предлагают пройти специальные экзамены производителя, которые уважают во многих организациях. Это не исчерпывающий список, и, определенно, существует множество других производителей, которые предлагают отличное образование и экзамены.

Если хотите узнать подробнее о сертификатах в области информационной безопасности, прочтите мою колонку в *InfoWorld*: http://www.infoworld.com/article/3115344/security/essential-certifications-for-smart-security-pros.html.

Методы Подготовки

Существует не меньше способов обучения, чем предметов обучения. Следующие разделы описывают самые распространенные способы.

Онлайн-подготовка

Практически не существует тестов, сертификатов или тем, которые нельзя освоить через онлайн-обучение. Это могут быть просто обучающие видео или обучение с полным погружением, на основе статей, видео, разбора глав и тестирования на профпригодность. Многие занимаются на уроках преподавателей, которые проводят обучение в реальном времени, где можно поднять цифровую руку и задать вопросы. Кто-то предпочитает обучение с реальным преподавателем, в обычном классе, но онлайн-обучение все чаще дает такой же опыт, и, как правило, за значительно меньшие деньги.

Взломай Мой Веб-сайт

Существует множество образовательных сайтов, которые созданы с целью их законного взлома. Это отличный способ обучить навыкам и позволить начинающим хакерам почувствовать волнительный момент взлома, без последствий, угрожающих тем, кто взламывает нелегально. Один из моих любимых сайтов подобного рода - это https://www.hackthissite.org/.

Школы и Подготовительные Центры

В наше время существует немного университетов, колледжей, технологических институтов или школ формального образования в которых нет программы подготовки по информационной безопасности. Несмотря на то, что обучение в таких заведениях стоит дороже, чем используя другие варианты, и вам необходимо заранее перепроверить, что вас не будет ждать бессмысленная болтовня, нацеленная на то, чтобы вытянуть из вас кровно-заработанные (например, фабрики дипломов, которые, на самом деле, не готовят вас к хорошей работе), такие учебные заведения часто предлагают основательное и всестороннее обучение безопасности. Многие профессионалы в области информационной безопасности начинают с технологических институтов или

местных колледжей, и, в конечном итоге, становятся выпускниками серьезных учебных заведений, с четырехлетним периодом обучения.

Учебные Лагеря (Boot Camps)

Учебные лагеря обеспечивают ускоренную подготовку, как правило, они фокусируются на получении определенной сертификации. Например, двухнедельная подготовка в учебном лагере может позволить получить сертификаты, которые выдаются за двух- или трехгодиченое обучение в технологическом институте. Мне нравятся учебные лагеря, я даже обучался в некоторых из них. Те, кто собирается заниматься в учебном лагере, должны быть готовы к интенсивному обучению, и они должны быть способны усваивать огромное количество информации за короткий промежуток времени. Для многих занятых людей учебные лагеря - это лучшая альтернатива для получения обращования. Нужно только убедиться, что учебный лагерь предоставляет гарантии возврата денег или прохождение нескольких тестов на получение сертификата.

Корпоративное Обучение

Как уже было сказано в разделе "Темы подготовки по информационной безопасности", многие организации предоставляют и даже требуют прохождения обязательного обучения по информационной безопасности. Многие крупные компании предлагают частичную или полную компенсацию затрат на обучение и проводят собрания, посвященные определенным темам или сертификатам по безопасности, которые ведут сотрудники. Многие соискатели считают преимущества корпоративного образования одним из главных, факторов для устройства в определенную компанию.

Книги

Конечно, глава, посвященная образованию, не была бы полной без упоминания того, что книги - это отличная возможность обучаться дома. В книгах, посвященных информационным технологиям, в основном, стараются максимально подробно раскрыть тему, и они, как правило, профессионально отредактированы с точки зрения технических деталей и грамматики.

Продолжительное соответствующее обучение одинаково необходимо для конечных пользователей, IT-персонала и специалистов по информационной безопасности. Одна из общих черт всех людей, у которых я беру интервью в этой книге - это то, что они постоянно учатся, а самые лучшие каждый день выделяют время на изучение чего-то нового.

Глава 42. Профиль: Стивен Норткатт

Я знаю Стивена Норткатта уже почти 20 лет. Он является не только важной частью невероятной организации, подготавливающей специалистов в сфере информационной безопасности SysAdmin, Networking, and Security Institute (SANS), но он также является одной из ключевых фигур в индустрии. Не помню сколько было случаев в моей писательской карьере, когда мне нужно было с кем-то поговорить, и все, что я делал - звонил Норткатту, и он организовывал встречу. Иногда кажется, что он производит впечатление практически на всех, кого встречает.

Норткатт сверхдружелюбный и рассудительный организатор. У него всегда есть отличные идеи, и он умеет мотивировать других пойти и реализовать свои планы. У некоторых людей есть особая харизма, которая притягивает других и побуждает к действию. Норткатт именно такой человек, и я уверен, что именно поэтому SANS взяли его в то время, когда они еще были крохотной организацией. Норткатт также является одним из первых инвесторов очень прибыльных компаний нашего времени, занимающихся информационной безопасностью, включая Tenable (http://www.tenable.com) и Sourcefire.

Организация SANS Institute (http://www.sans.org) была основана в 1989-ом, и с самого начала, у них были лучшие курсы по информационной безопасности. Их первоначальные конференции, посвященные безопасности, превратились в уважаемые в индустрии сертификаты, а их сертификаты превратились в аккредитованный учебный курс, предлагающий две программы по подготовке магистров (по технике обеспечения информационной безопасности (Information Security Engineering, MSISE) и управлению информационной безопасностью (Information Security Management, MSISM)) и три сертификата последипломного образования (Тестирование на проникновение и этичный взлом, реагирование на инциденты, а также техника обеспечения кибербезопасности). Они обучили более 100 000 человек, и у них работают самые востребованные преподаватели, многие из которых авторы бестселлеров. Если, будучи сотрудником компании, вы встретите сотрудника, у которого есть сертификат SANS, знайте, он лучший из лучших. Я считаю, что их новостные рассылки обязательны к прочтению для всех профессионалов по информационной безопасности, а их раздел Internet Storm Center одним из первых обнаруживает новые виды атак.

Несмотря на то, что я знаю Норткатта почти двадцать лет, я никогда не спрашивал, как он попал в сферу информационной безопасности, так что я спросил. Он ответил: “Я работал проектировщиком сетей в лаборатории

исследований ВМФ на рабочей станции Sun. Я ничего не знал об информационной безопасности. Однажды я обнаружил, что кто-то взломал мой компьютер. Это вывело меня из себя. Ко мне подключились из Австралии и на моей машине компилировали программу. Я не знал, что делать, поэтому просто выдернул кабель. Это были мои мероприятия по реагированию. После я чувствовал себя сильно оскорбленным. Я начал изучать информационную безопасность, и, в конце концов, получил финансирование. В то время, при наличии хорошей идеи, было несложно получить финансирование. Я многое узнал об информационной безопасности и, в конечном итоге, стал работать заместителем Фреда Кирби (более 16 лет Фред Кирби был менеджером информационного обеспечения в центре надводных сил ВМФ, дивизия Дальгрена, а сейчас он преподает в SANS).

Меня сильно заинтересовало обнаружение вторжений. Я создал систему обнаружения вторжений Shadow, которая в то время была очень эффективной. Я собрал команду по обнаружению вторжений, и, в итоге, мы проводили мониторинг более 30 военных баз (в конечном счете, он стал работать руководителем отдела информационной борьбы в организации по созданию обороны от баллистических ракет). Я совершил радикальную ошибку, приняв должность, которую мне предложили в Пентагоне. Я ушел из места, где был экспертом по технической части, в место, где я вообще не занимался техническими деталями. Моя работа заключалась в том, чтобы ходить на встречи и подписывать бумаги. Я занимался этим год. Это было в 1999-ом".

Несмотря на то, что Норткатт не был одним из сооснователей SANS (это были Мишель Гелл, Доктор Юджин Шульц, Алан Поллер и Доктор Мэтт Бишоп), он с самого начала часто пересекался с Аланом. Я спросил, как он начал работать в SANS. Он сказал: "В 1999-ом, я был козлом отпущения, которого запрягли работать в специальном проекте Пентагона по проблеме 2000 года, из опасений, что хакеры могут ее использовать. Я создал отличную команду, в которой были, в том числе, и лучшие технические аналитики со всего мира. Мне нравилась эта работа, но вопросы управления были сильно связаны с политикой, и это мне не нравилось. Затем пришел Алан (Поллер) и стал заниматься политическими вопросами, а я мог сосредоточиться на технической части. Я пришел обучаться на замечательную конференцию SANS по обнаружению вторжений в декабре 1999-го. Помню, что мне это нравилось гораздо больше, чем заниматься политикой. Так что я вернулся в свой офис в Пентагоне, собрал вещи, и не жалел о принятом решении.

Официально я начал работать в SANS 5-го января 2000 года. В то время они проводили только два мероприятия: весной и осенью. Каждое мероприятие длилось четыре дня. Перед главной конференцией проходили образовательные курсы, главная конференция длилась два дня, а после нее был еще один день, посвященный курсам подготовки. Это было замечательно, но я помню, как

сказал Алану: “Слишком много работы для всего двух мероприятий”. Так что их количество увеличилось”.

Я ходил на некоторые ранние курсы SANS задолго до того, как появились сертификаты. Я помню, что каждый из этих курсов был лучшим по своей теме, даже на сегодняшний день. Я помню кто их вел, и чему я научился. Я даже брал курс по Snort, инструменту обнаружения вторжений, у создателя этой программы Мартина Роеша в 1998-ом или 1999-ом. Когда я поделился с Норткаттом своими воспоминаниями, он сказал: “Я помню, как Марти подошел ко мне… будучи молодым парнем… и сказал: “Я создал новый инструмент по обнаружению вторжений, и он лучше, чем Ваш (Shadow)”, и он был прав. В итоге, я был одним из первых, кто инвестировал в смелый коммерческий проект Марти, который назывался Sourcefire”. Sourcefire был настолько успешным, что позже его купили Cisco.

Я спросил Норткатта, когда появилась идея перехода от подготовки к сертификатам. Он сказал: “Это была идея Алана. Я сразу понял, что он имеет ввиду, когда он говорил о том, что компании хотят быть точно уверены, что их деньги на подготовку специалистов потрачены не зря, и сертификаты были одним из вариантов предоставить такую уверенность. Помню, когда я еще работал в лаборатории ВМФ, я отправлял людей на конференцию Unix LISA. Я пришел на эту конференцию и не смог их найти. Оказалось, что они занимались каякингом в океане. Так что я понял важность сертификатов.

Идея курсов по сертификации появилась еще раньше. В 1998-ом Алан пришел ко мне в лабораторию ВМФ и поспорил со мной, кто сможет назвать больше направлений в сфере информационной безопасности. В то время их было немного: системы обнаружения вторжений, файрволы, обнаружение вредоносного ПО и некоторые другие. Поэтому, когда мы начали говорить о сертификатах, мы оба думали, что если образование и курсы будут специализироваться на конкретных задачах, то это обеспечит наилучший подход. В конце концов, мы создали более комплексный сертификат по основам безопасности GIAC Security Essentials Certification (GSEC), который, как бы является нашей версией CISSP. Сертификат GSEC не фокусируется на технической части. Он на километр шире и на пять сантиметров глубже. Но мы решили, что сначала людям необходимо дать понять основы безопасности, а потом давать им задачи, связанные с конкретной предметной областью, где полно командных строк”.

Когда мы закончили интервью, я вспомнил одну из наших первых встреч. У Норткатта была отличная идея - он хотел, чтобы я прилетел к нему домой на Гавайи. Я сказал, что проведу всю неделю, опустив голову вниз, потому что мне нужно закончить мою первую книгу (Malicious Mobile Code (https://www.amazon.com/Malicious-Mobile-Code-Protection-Windows/dp/156592682X)). Я уже сильно провалил дедлайн, и мне нужна была эта неделя, чтобы, наконец, закончить книгу и отнести ее издателю. Но он был

настойчив. Я отчетливо помню, что он сказал, как будто это было вчера. Он сказал: “Эй, вы с женой любите нырять с аквалангом, так? В общем, тут мой сосед, с которым дружим, собирается на Dive Hawaii, так что я дам тебе и твоей жене возможность отлично понырять”. Я снова поблагодарил его и сказал, что не могу выделить время, чтобы прилететь на Гавайи, встретиться и понырять. Он парировал: “Как зовут твою жену, дай мне ее номер? Я позвоню ей, расскажу об этой возможности и посмотрим, что она скажет!” Я не сказал ему, как ее зовут, и не дал ее номер, я не полетел на Гавайи, и, наконец, закончил свою первую книгу. Но я все еще жалею о том, что тогда не согласился. Вот такой он человек - вы навсегда запоминаете даже те его предложения, от которых отказываетесь.

Подробнее о Стивене Норткатте

Подробнее о Стивене Норткатте вы можете найти на этих ресурсах:

- Профиль Стивена Норткатта в LinkedIn: https://www.linkedin.com/in/stephenraynorthcutt
- Профиль Стивена Норткатта в SANS: https://www.sans.org/instructors/stephen-northcutt
- Профиль Стивена Норткатта на Facebook: https://www.facebook.com/stephen.northcutt
- Книга *Network Intrusion Detection* (в соавторстве с Джоди Новак): https://www.amazon.com/Network-Intrusion-Detection-StephenNorthcutt/dp/0735712654

Глава 43. Конфиденциальность

Многие, включая автора этой книги, уверены, что неприкосновенность частной жизни, особенно в цифровом веке, должна с рождения гарантироваться всем людям. К сожалению, цифровой и финансовой конфиденциальности давно не существует. Поисковые системы, рекламные сервисы и производители ПО часто знают о вас больше, чем кто-либо еще. Несколько лет назад, разъяренный отец пришел в магазин Target, потому что их рекламный отдел отправлял нежелательную рекламу с товарами для новорожденных его дочери-подростку. В конце концов, ему пришлось извиниться, когда он узнал, что Target знали о его дочери больше, чем он сам (http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-herfather-did/#d84bcce34c62).

В большинстве стран, особенно, когда дело касается интернета, конфиденциальность отсутствует. Ни одно ваше действие не остается незамеченным. Даже инструменты, гарантирующие сверхнадежную конфиденциальность, такие как Tor и "darknet", на самом деле, не так хороши. Не верите мне? Спросите у арестованных преступников, которые думали, что Tor или другой сервис гарантирует абсолютную анонимность. Существует множество способов быть менее заметным, но до тех пор, пока отслеживание ваших действий легально, компании (и правоохранительные структуры) будут за вами следить.

Это не означает, что некоторые государства и компании не пытаются предоставить приемлемый уровень конфиденциальности. Например, недавно вступивший в силу закон ЕС о защите персональных данных (https://en.wikipedia.org/wiki/General_Data_Protection_Regulation) позволяет штрафовать компании на сумму до 4% от их оборота за его нарушение. В большинстве стран существует закон (или несколько законов), направленный на защиту частных данных граждан.

К сожалению, большинство законов - это полумеры, которые, в первую очередь, направлены на защиту государств и бизнес-организаций, собирающих частные данные, а не на защиту конфиденциальности пользователей. А во многих странах, особенно Азиатско-Тихоокеанского региона, прямо отклоняют любые законы, которые не позволяют государству вести тотальную слежку за гражданами. Культурные нормы в этих странах таковы, что большинство граждан часто воспринимает это без каких-либо жалоб. Они разменивают конфиденциальность на мнимую безопасность. Как правило, в странах, в

которых никогда не пытались обеспечить конфиденциальность граждан, вести тотальную слежку не составляет труда.

Тем не менее, нарушение государственных законов о конфиденциальности может дорого стоить нарушителям. Правительственные департаменты и целые правительства признавались виновными в нарушении существующих законов о конфиденциальности (хотя, почти никогда не наказывались). С другой стороны, бизнес-организации могут легко попасть в неприятную ситуацию. Все чаще в корпорациях появляются подразделения по защите конфиденциальных сведений, которые занимаются защитой частных данных пользователей.

Организации, Занимающиеся Вопросами Конфиденциальности

К счастью для всего мира, существует множество организаций, которые борются за право на конфиденциальность всех граждан на планете. В том числе Фонд электронных рубежей (Electronic Frontier Foundation, EFF) (https://www.eff.org/) и Информационный центр по защите частной жизни в электронной среде (Electronic Privacy Information Center, EPIC) (https://epic.org/).

Фонд электронных рубежей (EFF) был основан в 1990-ом, чтобы продвигать прозрачность действий правительства, конфиденциальность пользователей и свободу слова по всему миру. Они делают это с помощью сочетания судебных разбирательств, демонстраций, анализа государственной политики, публикаций и создания технических инструментов. Они очень активно участвуют в нескольких судебных исках, включая случай, где они борются за право компаний заправлять и продавать чернильные картриджи производителей (https://www.eff.org/cases/impression-products-inc-v-lexmark-international-inc). Их инструменты для обеспечения конфиденциальности включают HTTPS Everywhere (https://www.eff.org/https-everywhere), расширение для браузеров Firefox, Chrome и Opera, которое позваляет обеспечить максимальное использование протокола HTTPS и расширение Privacy Badger, которое блокирует рекламу и другие инструменты отслеживания.

Информационный центр по защите частной жизни в электронной среде (EPIC) это некоммерческая исследовательская организация, основанная в 1994-ом, которая специализируется на защите конфиденциальности, свободы слова, гражданских прав и других демократических ценностей, она активно использует судебные разбирательства, публикации и другие правозащитные инструменты. EPIC использует судебную систему даже больше, чем EFF, и обе организации выступают за улучшение кибербезопасности, но при этом они понимают важность других своих целей, которыми нельзя жертвовать в угоду кибербезопасности. На сайте EPIC есть огромный список проблем конфиденциальности (https://epic.org/privacy/).

Политические проблемы, описанные как EFF, так и EPIC, как правило, шокируют многих людей, которые раньше не сильно углублялись в детали. Поражает, какой огромной части конфиденциальности личных данных мы уже лишились. Почти ничего не осталось. Обе организации являются некоммерческими, созданными на основании раздела 501(c)(3), и существуют на пожертвования. Если вы действительно беспокоитесь о конфиденциальности и свободе слова, то задумайтесь о пожертвовании организации, выступающей за конфиденциальность.

Отдельная благодарность выражается Брюсу Шнайеру (https://www.schneier.com/) за его неустанные усилия научить нас и защитить частные данные. Шнайер публично высказывался против разрушения конфиденциальности, а его книги, особенно *David and Goliath* (https://www.amazon.com/Data-Goliath-Battles-Collect-Control/dp/039335217X/) обязательно должны прочитать те, кто хочет знать, на каком уровне наша конфиденциальность находится в данный момент и куда все идет. Подробнее о Брюсе Шнайере можно прочитать в 3-ей главе.

Приложения для Защиты Конфиденциальности

Ни одно из предыдущих ужасных предупреждений о том, что наши частные данные становятся все более доступными, не должно истолковываться, как утверждение. Что ничего нельзя сделать для повышения защиты личных данных. Существует множество замечательных, бесплатных приложений, которые могут дать вам максимально возможную защиту конфиденциальности, и оказывают минимальное влияние на комфорт использования. Практически любой сторонник конфиденциальности посоветует использовать Tor (https://www.torproject.org/), чтобы значительно усложнить вторжение в вашу личную жизнь всех, кроме организаций с огромными ресурсами. Tor не обеспечивает идеальный уровень конфиденциальности, но это лучший инструмент общего назначения, который у нас есть. Многие сторонники неприкосновенности частной жизни любят использовать поисковую систему DuckDuckGo (https://duckduckgo.com/), вместо других поисковых систем, которые финансируются с целью вторжения в личную жизнь. Многие производители ПО соревнуются в обеспечении максимально возможной конфиденциальности. Чтобы подробнее ознакомиться с программами, обеспечивающими конфиденциальность, пожалуйста, прочтите о приложениях, которые выбрал автор: http://www.infoworld.com/article/3135324/security/17-essential-tools-to-protect-youronline-identity-and-privacy.html.

У нас не может быть безопасности и свободы без защиты личных данных. В следующей главе мы поговорим о Еве Галперин, которая работает в фонде электронных рубежей.

Глава 44. Профиль: Ева Галперин

Вы должны полюбить человека, который увлекается компьютерами и кибербезопасностью, а свободное время занимается воздушной акробатикой в цирке, в качестве хобби. Директор по кибербезопасности фонда электронных рубежей (https://www.eff.org) Ева Галперин именно такой человек. Работая на EFF с 2007-го, она стала директором по кибербезопасности в 2017-ом. До работы в EFF она получила степени по политологии и международным отношениям в Университете штата Калифорния в Сан-Франциско. В основном, ее работа фокусируется на обеспечении конфиденциальности, свободы слова и безопасности для всех жителей планеты, а также анализе вредоносного ПО, которое угрожает всем нам. Сейчас Галперин известна по всему миру за ее работу "в поле", описание вредоносного ПО, с которым она столкнулась и выступления на таких конференциях, как BlackHat (https://www.blackhat.com/us-16/speakers/Eva-Galperin.html).

Я спросил Галперин, как она попала в сферу информационной безопасности, и она ответила: "Я довольно рано начала интересоваться компьютерами. Мой папа был специалистом по информационной безопасности, и я попросила его разрешить мне "позависать" на Prodigy (предшественнике AOL, и других онлайн-сервисов). Вместо этого он создал для меня отдельный рабочий стол на своем компьютере на базе Unix/Solaris. 12-летний ребенок… за компьютером на базе Unix, представляете? На платформе Usenet я участвовала в общении на тему научно-фантастических книг, играла в интерактивные текстовые игры, а когда появился веб, я стала интересоваться созданием веб-страниц. В колледже я была администратором Unix-систем, и в то время, системное администрирование включало обеспечение информационной безопасности.

Я спросил, как она попала в EFF и стала заниматься анализом вредоносного ПО. Она сказала: "Я пришла в EFF в 2007-ом в качестве активистки. В итоге, я проводила исследования кибербезопасности, потому что больше никто в EFF этим не занимался. Мои исследования вредоносного ПО начались в 2011-ом в Сирии. В то время (сирийский президент Башар Хафез аль-) Асад был любимчиком Запада. Он позиционировал себя, как отец сирийского интернета, и открыл доступ к Facebook, который ранее был заблокирован. Западные страны думали, что разблокировка Facebook была признаком того, что Асад увеличивал открытость и свободу слова. Они очень сильно ошибались. На самом деле целью разблокировки были MITM-атаки. Я занималась Сирией и проводила исследование проблем цензуры и свободы слова, когда кто-то обнаружил вредоносное ПО, созданное сторонниками Асада, и целью этого ПО

были те, кто поддерживал оппозицию. На их машины была установлена троянская программа удаленного доступа (Remote Access Trojan, RAT) и она передавала данные, включая пароли и скриншоты на сирийский IP-адрес. Вместе, мы проанализировали эту программу. В течение следующих двух лет я помогла написать с десяток отчетов о двух группах, поддерживающих Асада, которые создавали это вредоносное ПО".

Я спросил Галперин, что, по ее мнению, является наибольшей проблемой в сфере информационной безопасности. Она ответила: "Самая большая проблема информационной безопасности не в безопасности. А в конфиденциальности. Многие компании делают приоритетной безопасность информации, но не защищают частные данные своих пользователей. У многих компаний есть огромное количество максимально подробной информации о пользователях и как только она появляется у этих компаний, она становится объектом легального взлома (повестки в суд и судебные распоряжения), и, в то же время, объектом технических атак, которые обычно стараются предотвратить ребята из информационной безопасности. Даже если компания защищает эти данные от хакеров, их гораздо сложнее защитить от правительства или правоохранительных структур. Как правило, компании даже не рассматривают правительство или правоохранителей в качестве атакующих. Я хочу, чтобы меня правильно поняли, я не пытаюсь сказать, что компании не должны собирать никаких данных, но у пользователей должна быть возможность контролировать свои данные. Пользователь должен знать, когда, что, как было собрано, как долго это будет храниться, каким будет уровень безопасности, и так далее. Выбор пользователя невероятно важен".

Учитывая ее знания о работе правительства в разных странах, я поинтересовался, как она оценивает правительство США с точки зрения обеспечения защиты частных данных по шкале от одного до 10, где 10 - это наилучшая оценка. Она сказала: "С точки зрения защиты частных данных, США я бы поставила 4 или 5. Самая лучшая защита цифровой конфиденциальности в ЕС. С другой стороны, в США гораздо больше свободы слова, в то время как в ЕС нет таких сильных механизмов по ее защите".

Я спросил, что, по ее мнению, произойдет с конфиденциальностью и свободой слова. Она ответила: "Легко сказать, что все станет хуже. Можно так сказать, и, когда это случится, чувствовать себя гением. Но я выбираю другую тактику. Я думаю, что существует возможность улучшения ситуации, но пока информация пользователей является товаром, а свободное ПО или сервисы - это то, на что они меняют этот товар, будет очень сложно изменить что-то к лучшему. Мы знаем, что пользователи действительно ценят конфиденциальность, и часто готовы за нее заплатить, если предоставить им выбор. Но нужно дать им этот выбор, а я не уверена, что это произойдет, потому что крупные игроки становятся только сильнее, и такое действие никак не укладывается в текущую бизнес-модель".

Напоследок, я должен был спросить Галперин, как она начала увлекаться воздушной акробатикой. Она ответила: “В средней школе я занималась гимнастикой. В моей старшей школе была цирковая секция, поэтому вместо обычного спорта, я стала заниматься акробатикой. После старшей школы, я делала несколько упражнений из воздушной акробатики и снова чувствовала себя на 20. Это отличные упражнения, а когда вы крутитесь на высоте 9 метров, то не думаете об интернете”.

Не знаю, как вы, а мне нравится осознавать, что один из самых известных сторонников конфиденциальности не боится рисковать, ни в своей работе, ни в своем хобби.

Подробнее о Еве Галперин

Подробнее о Еве Галперин вы можете найти на этих ресурсах:

- Твитер Евы Галперин: https://twitter.com/evacide
- Профиль Евы Галперин в EFF: https://www.eff.org/about/staff/eva-galperin

Глава 45. Установка патчей

Каждый день миллионы веб-сайтов и электронных писем содержат вредоносные ссылки на “наборы эксплойтов”. Программисты (или команды программистов), создающие вредоносное ПО используют или продают наборы эксплойтов. Как правило, в наборах эксплойтов есть все, что нужно тому, кто мечтает стать хакером, включая техподдержку 24/7 и автообновления, которые позволяют избежать обнаружения антивирусными сканерами. Хороший набор эксплойтов может даже найти и сделать вредоносным веб-сайт, который до этого был безопасным. С помощь него в дальнейшем можно заразить пользователей, которые позже зайдут на этот веб-сайт. Все, что нужно сделать злоумышленнику - купить такой набор, запустить его и отправить на поиски сайтов-жертв.

Почти всегда набор эксплойтов содержит клиентскую часть (программы, запускаемые на компьютерах конечных пользователей, в зависимости от вредоносного кода, который взламывает серверы), которая осуществляет проверку на отсутствие многочисленных патчей. Такие программы могут осуществлять проверку на наличие как небольшого количества уязвимостей, так и нескольких десятков. Неудачливые посетители, которые не устанавливали патчи, подвергаются незаметному взлому (также известному, как “drive-by download”), в то время, как к посетителям, использующим пропатченное ПО, как правило, применяется социальная инженерия, их стараются убедить установить троянскую программу. Обычно плохие парни, использующие наборы эксплойтов, стараются взломать непропатченные устройства, а не применять социальную инженерию, потому что не все пользователи по умолчанию согласятся установить ту программу, которую им предлагают. В большинстве наборов эксплойтов есть даже консоль централизованного управления, с помощью которой преступники могли видеть, какие уязвимости используются и как заражаются устройства.

Но даже без наборов эксплойтов, отсутствующие патчи - одна из главных проблем, способствующих взлому. Возможно однажды все изменится, но уже почти три десятилетия это остается фактом. Все, что нужно сделать, чтобы обеспечить на компьютерах наилучшую защиту от уязвимостей ПО – это своевременно и постоянно устанавливать обновления безопасности. Звучит не сложно. Есть даже десятки инструментов, которые могут в этом помочь.

К сожалению, своевременная установка патчей остается слишком сложным и труднодостижимым идеалом. Не уверен, что за всю свою карьеру сканирования сотен и сотен тысяч компьютеров, я хотя бы раз видел компьютер, на котором

были установлены все патчи. А если и видел, то не вспомню. Такое случается довольно редко.

Зачем Обновлять Устройства?

В следующих разделах описаны самые значимые факты, которые упускаются из виду большинством пользователей.

Большинство Эксплойтов Используют Старые Уязвимости, для Которых Существуют Патчи

Для взлома большинства устройств вредоносное ПО использует уязвимости, которые были исправлены патчами выпущенными год назад или более. Многие исследования показывают, что, как правило, используются те уязвимости, которые закрываются патчами, выпущенными производителем два или три года назад. Существует немалый процент компьютеров, на которые совсем не устанавливают патчи. Если включить в файрволе функцию поиска и обнаружения вредоносных программ, которые пытаются заразить ваш компьютер или сеть, то можно обнаружить эксплойты, которые были эффективны более 15 лет назад (например, Code Red, SQL Slammer, и так далее). Иногда встречаются уязвимости нулевого дня (угрозы, использующие уязвимости, для которых не выходили патчи), но они встречаются редко и, в основном, составляют менее 1% всех успешных атак в интернете.

Большинство Эксплойтов Используют Только Несколько Непропатченных Программ

В среднем, за год, в сотнях различных программ обнаруживается 5000 - 6000 отдельных уязвимостей. Но, как правило, целью взлома является только несколько программ. Например, в отчете *Cisco 2014 Annual Security Report* (http://www.cisco.com/web/offers/lp/2014-annual-securityreport/index.html) говорится, что 91% всех взломов домашних компьютеров через интернет приходится на непропатченную программу Oracle Java. Если добавить сюда топ-4 остальных программ, то все они будут составлять 100% всех успешных взломов через интернет. То есть, тот, кто установит обновления безопасности для пяти программ, значительно снизит риск взлома в любой среде. Java больше не является основной программой, через которую производится взлом. Этого результата добились благодаря совокупности факторов (в том числе, отказ основных производителей браузеров от совместимости с Java по умолчанию), но программа номер один, которая больше всего подвержена взлому, всегда меняется. Много лет назад такой программой была DOS, затем

Microsoft Windows, Microsoft Outlook или Microsoft Internet Explorer. Сегодня, такими программами, в основном, являются расширения браузеров, потому что они, как правило, работают на нескольких платформах. Программы, которые больше всего подвержены взлому могут меняться, но факт наличия нескольких программ, которые больше всего подвержены взлому, вряд ли потеряет свою актуальность в ближайшем будущем.

Программы, для Которых Реже Всего Устанавливаются Патчи, не Всегда Являются Целью Взлома

Существует огромная пропасть между вероятностью заражения программ, для которых патчи устанавливаются реже всего, и непропатченных программ, с помощью которых, чаще всего осуществляется взлом. Хороший эксперт по информационной безопасности понимает эту разницу, и концентрирует усилия на последних. Например, Microsoft Visual C++ Redistributable долгое время была программой, которую устанавливали сторонние программы, и для которой реже всего устанавливались патчи. Однако, ее практически не взламывали, потому что сторонние программы устанавливали и использовали ее по-разному, что затрудняло обнаружение и использование уязвимости. Защитники должны фокусироваться на установке патчей для устранения дыр в безопасности тех программ, которые чаще всего взламывают. А это не всегда популярные программы, для которых редко устанавливаются патчи.

Необходимо Патчить и Аппаратные Компоненты

Как правило, аппаратные компоненты имеют собственную прошивку. Прошивка - это, по сути, программа, установленная в кремниевый чип, или, как я люблю их называть, "программы, которые сложнее обновить". Специалисты по информационной безопасности должны устанавливать патчи на аппаратные компоненты, прошивку, BIOS, и любое оборудование имеющее собственное ПО.

Основные Проблемы при Установке Патчей

Если бы устанавливать патчи было легко, то это не являлось бы такой проблемой, какой является сегодня. В следующих разделах описаны некоторые проблемы, связанные с установкой патчей.

Проверка Неустановленных Патчей не Всегда Дает Точный Результат

Неважно, какую программу вы используете для проверки наличия новых патчей, она может показать не все доступные обновления. Во многих случаях в этом виновата не сама программа, отвечающая за установку обновлений. Компьютерные устройства - это сложные машины, с большим количеством заменяемых элементов, в которых присутствует много багов, и любой из этих багов может помешать проверке наличия обновлений. Более того, пользователи могут работать с устройствами или версиями устройств, которые не поддерживаются вашей программой, проверяющей наличие патчей, или вам могут помешать границы безопасности сети. Существует огромное количество причин, по которым результат проверки обновлений может быть неточным. Такая проверка никогда не дает 100% точность. А если невозможно обнаружить наличие новых патчей, то вам не получится их установить.

Невозможно Всегда Устанавливать Патчи

Java компании Sun (а теперь Oracle) долгое время оставалась самой взламываемой программой. Для исправления этой ситуации было необходимо установить патчи, но, к сожалению, большая часть пользователей по всему миру не устанавливала их почти двадцать лет. Программисты Java постоянного пишут свои программы, опираюсь на определенную версию Java, и ее возможности, и после обновлени эти программы могли перестать работать. Из-за того, что многие программы в компаниях были написаны на Java, а она была основной причиной взлома, компаниям приходилось с этим жить, они не могли устанавливать патчи. Оказалось, что те, кто стал причиной сбоев в работе, резко увеличивали свои шансы на увольнение, по сравнению с теми, кто просто сообщал о невозможности установки патча, так как владелец бизнеса запрещал обновляться.

Существует Определенный Процент Компьютеров, на Которые не Устанавливаются Патчи

По тем же причинам, которые мешают точной проверке обновлений, существует небольшой процент компьютеров, на которые не устанавливаются патчи. По моему опыту, таких компьютеров не много, в среднем 1-2%, но иногда эта цифра может доходить до 15-20%, в зависимости от сложности патча и самих устройств. Один из лучших способов решить проблему с установкой патчей - это отслеживать и исправлять компьютеры, которые не определяются при проверке обновлений, и имеют проблемы с их установкой.

Установка Патча Приводит к Сбоям в Работе

Производители делают все возможное, чтобы снизить количество сбоев, вызванных установкой обновления, но они не могут протестировать патч на всех возможных комбинациях "железа" и программ. В некоторых случаях установка надежного и безопасного патча может быть прервана вредоносной программой, которая ранее не была обнаружена или непротестированной сторонней программой. Многие компании "обожглись" на установке одного или нескольких патчей, вызвавших серьезные сбои в работе, и теперь не устанавливают патчи без проведения многочисленных тестов (на которые у них, как правило, не хватает времени или ресурсов). Из-за опасения непредвиденных сбоев в работе, они либо совсем не устанавливают патчи, либо не устанавливают их вовремя. Я понимаю эти опасения, но отсутствие своевременных критических обновлений безопасности приводит к большему риску, чем менее вероятные сбои в работе. Если вы беспокоитесь о возможных сбоях в работе, то просто подождите несколько дней. В большинстве случаев, такие проблемы обнаруживают те, кто быстрее устанавливают обновления, и после того, как производитель их решит, можно безопасно установить патч.

Выход Патча - Это Официальный Анонс Всему Миру о Наличие Уязвимости

Если об определенной уязвимости не было известно ранее, то с выходом патча, призванным ее устранить, все меняется. Создатели вредоносного ПО и наборов эксплойтов быстро анализируют любой новый патч и осуществляют реверс-инжениринг, с помощью которого они стараются узнать, как можно использовать обнаруженную уязвимость. Так как даже самые лучшие патчи устанавливаются спустя несколько дней, а некоторые пользователи совсем их не устанавливают, выход нового патча открывает новые перспективы для взлома.

Некоторые производители прячут исправление критических уязвимостей в патчах, которые призваны решить другие проблемы, и не сообщают об этом. Затем, они официально заявляют о наличие такой уязвимости и выпускают соответствующий патч. К тому моменту, благодаря предыдущему патчу, данный баг уже был исправлен на большинстве компьютеров. Был случай, когда один популярный разработчик ОС исправлял критическую уязвимость, выпуская патчи в течение нескольких месяцев. Для тех, кто занимается реверс-инжинирингом это выглядело, как непонятные, "мусорные" сегменты кода, но после трех месяцев установки патчей, был исправен весь баг, который представлял собой огромную дыру, оставив клиентов счастливыми, а хакеров в недоумении.

В итоге, грамотная организация обновлений - это своевременная, постоянная установка патчей программ, которые являются наиболее вероятным объектами взлома. Это легко сказать, но сложно сделать. Я рекомендую включить все автообновления или использовать соответствующую, надежную программу, которая будет обновлять все ПО (и, по возможности, ПО аппаратных компонентов), и устанавливать критические обновления безопасности в течение нескольких дней. Если вы будете устанавливать патчи в течение нескольких дней после их выхода, то вы сильно обезопасите свою среду в интернете. Идеальная организация обновлений может быть нелегкой задачей, но установка патчей, исправляющих критические уязвимости в программах, которые больше всего подвержены взлому, обязательна на каждом компьютере. Те, кто этого не делают, так и просят, чтобы их взломали.

В следующей главе мы поговорим о Уиндоу Снайдер, женщине, которая помогает крупнейшим компаниям в мире обновлять свои продукты.

Глава 46. Профиль: Уиндоу Снайдер

Уиндоу Снайдер работала на самые влиятельные компании индустрии. Поначалу она работала в @Stake в качестве директора архитектуры системы безопасности. @Stake была успешной компанией, которая специализировалась на поиске уязвимостей и информационной безопасности, и генерировала или приобретала больше, чем большинство суперзвезд компьютерной индустрии. В конечном итоге, она была куплена Symantec в 2004-ом. В 2002-ом Снайдер ушла работать в Microsoft, где была специалистом по вопросам стратегии безопасности в отделе обеспечения безопасности и связи. Она участвовала в создании SDL (Security Design Lifecycle) и в разработке новой методологии для программ по моделированию угроз. Она также отвечала за безопасность Microsoft Windows XP Service Pack 2, по сути, первой серьезной попытке Microsoft создать операционную систему, безопасную по умолчанию, а также за безопасность Windows Server 2003. Она занималась взаимоотношениями консалтинговых компаний по вопросам безопасности Microsoft, а также отвечала за развитие стратегии пропаганды в области информационной безопасности.

В 2006-ом она присоединилась к Mozilla и использовала шутливое название должности "главный сотрудник по вопросам чего-то там" вместо более формального "главный сотрудник по вопросам безопасности" (Chief Security Officer, CSO). Помню, многие из нас завидовали такой должности. В конце концов, она работала в Apple в качестве старшего менеджера по продуктам безопасности, и занималась разработкой стратегии и функций безопасности и конфиденциальности для iOS и OS X. Сейчас она работает в Fastly (https://www.fastly.com/), сети доставки контента, которая быстро расширяет свое влияние на другие сервисы, включая те, которые обеспечивают информационную безопасность. Вместе со своим соавтором Фрэнком Суидерски, она написала книгу *Threat Modeling* (https://www.amazon.com/Threat-Modeling-Microsoft-Professional-Swiderski/dp/0735619913/). Ее отец американец, а мать родом из Кении. Снайдер - единственный человек, с которым я знаком лично, который работал на три из четырех крупнейших компаний, разрабатывающих самые популярные браузеры и ПО. Скажем так, она работает на передовой.

В начале нашего интервью я должен был спросить о ее имени. Она ответила: "Я могу рассказать историю о том периоде, когда я работала в Microsoft. В то время, по умолчанию, email-адреса, как правило, начинались с имени человека, а затем шли инициалы. Но у огромной группы рассылки электронной почты, той

группы, которой отправлялись письма о продукции Windows, в качестве имени использовалось слово Windows (которое было бы моим логином электронной почты, если бы я использовала имя по умолчанию). На протяжении многих лет люди хотели отправить мне что-то личное или конфиденциальное… возможно информацию о вредоносном ПО или отчет о новой уязвимости, но вместо этого, они случайно отправляли эту информацию самой большой группе рассылки электронной почты. Вероятно, в конце концов, они осознавали свою ошибку, когда видели сообщение о невозможности отправить письмо, так как список адресатов заблокирован".

Затем я спросил, как она попала в сферу информационной безопасности. Она сказала: "Моей основной специальностью была информатика, и я заинтересовалась криптографией и криптоанализом. Меня интересовала идея секретов, ограниченных сложностью математического алгоритма. Примерно в то же время, я впервые получила доступ к многопользовательской операционной системе. Я стала задумываться о границах безопасности между различными пользователями и их действиями, а также о том, что не давало им мешать работе друг друга или работе операционной системы. Я обнаружила, что, в то время, в лучшем случае, были полупроницаемые барьеры. Было весело, это как разбирать паззл, точнее машину, и узнавать, как она работает. Это было интересное время".

Я знал, что она участвовала в разработке SDL (Security Design Lifecycle), когда работала в Microsoft. Я спросил, как она туда попала, и чем она там занималась. Она ответила: "Когда я впервые попала в Microsoft, это была совсем не та организация, которая знает толк в информационной безопасности. В соответствующем отделе работало где-то одиннадцать человек. Я была двенадцатой, и я занималась безопасностью Windows. И, в то время, моя работа, в основном, заключалась в реагировании на то, что обнаружили другие люди, не работающие в Microsoft. Тогда не было сильной внутренней программы. Затем "ударили" SQL Slammer и Blaster. Я была одним из создателей первой методологии официального моделирования угроз (она также является одним из соавторов книги на эту тему). Я помогла начать профилактический поиск багов и выйти на связь с сообществом пользователей. В то время, когда я только начала работать в Microsoft, если кто-то извне находил уязвимость безопасности, Microsoft называли его хакером. В то время СМИ ассоциировали хакеров всевозможными преступниками. Те, кто сообщал о проблемах в Microsoft, и даже публично выкладывал сведения о непропатченной уязвимости, не были преступниками. Я помогла продвинуть программу, с помощью которой нам удалось сделать их нашими союзниками, а не врагами. Одним из улучшений было то, что их стали называть исследователями безопасности, а не хакерами, так удалось подчеркнуть важность их работы. Я также помогла создать программу по финансированию многих небольших хакерских конференций, за пределами Microsoft, таких как

Hack-in-the-Box. В конечном итоге, мы смогли изменить убеждение, что Microsoft не волнует безопасность или что Microsoft ничего не понимает в безопасности. На самом деле исследователи безопасности и Microsoft были в одной команде.

Когда я впервые пришла в Microsoft, у них не было человека, отвечающего за безопасность продуктов Windows, поэтому я вызвалась. Я представляла безопасность Windows на встречах, на которых присутствовали спонсоры и совладельцы. У нас было огромное количество багов, которые мы пытались исправить в стиле "убей крота", и это было не эффективно. Как часть проекта SDL, мы стали изучать более глубокие причины появления багов, пытаясь обнаружить их происхождение, исправив которое, мы бы сразу избавились от множества багов. Мы взяли уроки, полученные при работе с командой по безопасности Windows, и передали их другим командам, чтобы они так же применяли их в других продуктах, таких как Microsoft Office".

Я попросил ее рассказать еще об одном уроке, который она выучила, и как она воспользовалась полученными знаниями. Она ответила: "Сегодня, за вредоносными программами стоит целая финансовая экосистема. Есть группа людей, которые ищут уязвимости, есть группа людей, которые добавляют эти уязвимости в наборы эксплойтов. Есть еще одна группа людей, которые хотят заразить как можно больше веб-сайтов и компьютеров, используя эти наборы, а есть еще одна группа людей, которая использует эти инструменты в своих целях. Но, если удалить одно звено из этой цепи, то остальным будет сложнее делать бизнес. Если можно совершить действия, которые сделают ключевые моменты экосистемы более дорогими или сложными в реализации, то это сильно усложнит работу всей цепочки. Microsoft и команда Windows не смогли вовремя это понять. Когда я пришла в Microsoft, они уже испытывали нашествие вредоносных программ, червей и вирусов. Затем я работала над другими платформами, включая iOS и OS X в Apple, и я использовала свой опыт, чтобы успешно установить "дорожные заграждения", которые усложняли работу экосистемы вредоносного ПО и делали ее менее прибыльной. Если можно подорвать экономическую выгоду вредоносного ПО, то этот способ тоже нужно использовать".

Снайдер работала в самых крупных и известных компаниях. Я спросил, что общего есть у таких разных корпораций. Она ответила: "Во всех компаниях нужно обеспечивать безопасность конечных пользователей. Слишком дорогие функции безопасности, которые сильно мешают работе пользователей, не получат одобрения. Мы должны улучшать безопасность, но это не должно мешать работе пользователей. Кроме того, не надо собирать данные, которые вам не нужны. Если вы собираете данные, то вы должны обеспечить их защиту, и дать пользователям возможность контролировать собственные данные. Самая главная проблема информационной безопасности - это успешная реализация на практике наших знаний".

Подробнее о Уиндоу Снайдер

Подробнее о Уиндоу Снайдер вы можете найти на этих ресурсах:

- Профиль Уиндоу Снайдер в LinkedIn: https://www.linkedin.com/in/window
- Твиттер Уиндоу Снайдер: https://twitter.com/window

Глава 47. Карьера Писателя

В старших классах я дважды завалил экзамен по письму. В магистратуре, во время прохождения практики организации больничного обслуживания, мой первый корпоративный отчет был написан настолько ужасно, что начальник стал громко задавать вопросы о всей системе образования в нашей стране. Когда я периодически его перечитываю, для того, чтобы вспомнить, с чего я начинал, я испытываю физическую боль. Спустя почти 30 лет я являюсь автором и соавтором девяти книг и почти 1000 статей в общенациональном журнале и уже 12 лет я работаю в качестве обозревателя сферы информационной безопасности в журнале *InfoWorld*. Все благодаря моему брату, собственной настойчивости и множеству редакторов.

При том, что я все еще не могу написать электронное письмо без опечатки, я значительно улучшил свое правописание и теперь зарабатываю этим деньги. Я часто пишу тексты, на которых могу заработать до $500-1000/час, и зарабатываю этим за год больше, чем среднестатистическая американская семья, и это только подработка. Хотя моя основная работа - консультант по информационной безопасности, писательской деятельностью я занимаюсь еще дольше. Это неплохой дополнительный доход, который я могу получить, когда пишу дома, в самолете и гостиничных номерах, в свободное время, после целого дня работы консультантом. Кто-то по ночам смотрит телевизор. Я обычно пишу, когда смотрю телевизор. Писательское хобби позволяет мне устроить хороший семейный отдых и тратить очень много денег на свои увлечения. Я не один такой.

Сотни людей по всему миру зарабатывают на книгах и статьях об информационной безопасности. Комфортно устроившись дома, с хорошим интернетом, они обеспечивают себя и свои семьи. Кто-то работает на признанных медиа-гигантов, остальные зарабатывают фрилансом, продавая свои статьи и услуги. Они все - фанаты информационной безопасности, которые фильтруют маркетинговую шумиху, созданную производителями и раскрывают глаза читателям на то, что действительно происходит.

Способы Публикации Работ по Информационной Безопасности

Существует множество способов опубликовать свою работу по информационной безопасности, включая те, что описаны ниже.

Блоги

Как правило, те, кто пишет, об информационной безопасности, постоянно ведут блог или участвуют в нескольких блогах. По сути, блоги - это современная версия статей в журнале. Посты в блогах могут оплачиваться или не оплачиваться, могут прорабатываться или не прорабатываться редакторами, которые исправляют ошибки, перед выходом поста. Сделать собственный сайт или начать вести блог легко, тем не менее, основные проблемы заключаются в том, чтобы привлечь читателей и не переставать писать в течение долгого периода. Подавляющее большинство блогов появляется и перестает существовать в течение одного года, так как авторы либо не набирают аудиторию, на которую "замахнулись", либо высказали все, что хотели. Блог, как и статьи в журнале, нелегко поддерживать на достаточно высоком уровне.

Если вы хотите завести собственный блог, и не знаете с чего начать, попробуйте самые популярные сервисы для создания блога, среди которых, абсолютный лидер - WordPress (http://www.wordpress.com). WordPress создан компанией Automattic, которая прекрасно понимает, что делает, с ее помощью создано 27% всех сайтов в интернете и, примерно, 70% всех сайтов для ведения блога.

Социальные Сети

Большинство экспертов по информационной безопасности используют Твиттер, в котором, время от времени (или ежедневно), постят твиты. Во-вторых, у многих есть профессиональные (или личные) профили на Facebook, LinkedIn или в Google Groups. У многих писателей есть профили во всех этих сервисах, а также отдельные сайты, где они выкладывают свои публикации.

Статьи

Многие профессионалы в сфере информационной безопасности пишут "статьи", которые, как правило, могут составлять от нескольких сотен до многих тысяч слов. В среднем, длина колонки составляет 1000 слов. Статьи могут быть опубликованы в печатных журналах, в онлайн-версиях или быть частью блогов. Заголовки статей могут относится к категориям новостей, мнений, практических пособий или технических обзоров.

Если вы любите писать, и вам повезет, то можно даже получить еженедельную или ежемесячную колонку. Однако, перед тем, как начать профессиональную карьеру писателя, убедитесь, что вы действительно этого хотите. Я помню, как был взволнован, когда получил колонку в журнале *InfoWorld* в августе 2005-го. Мне не терпелось рассказать всему миру все, что я думал и все, что меня интересовало. Оказалось, что можно рассказать всему

миру обо всем, что вас действительно интересует, примерно, за 12 статей. Затем нужно поймать ритм создания новых идей, каждый раз, когда приходит время написать колонку. Иногда, я просыпаюсь в 4 утра, и пишу три колонки. А иногда, мне сложно придумать новую, интересную статью или точку зрения, и я выхожу далеко за дедлайн. Многие писатели, которые работают с одной тематикой, "выгорают", так что, если хотите сделать карьеру писателя, найдите творческую тему, которая будет интересна вам и вашему нанимателю.

Книги

Книги - это отличный способ поделиться знаниями, и даже проверить собственные навыки писателя. Я все еще отчетливо помню радость от получения контракта на публикацию своей первой книги (после нескольких лет попыток, и более 100 отказов), и от ощущения, когда держал ее в руках. Если вы автор книги, то в вашем некрологе, скорее всего, будет написано "автор книги". Никто не сможет этого отнять.

Учитывая все вышесказанное, до тех пор, пока вы не найдете способ поженить международные заговоры, вампиров, зомби и информационную безопасность, желательно с главным героем-подростком, вы вряд ли будете богатым автором. Подавляющее большинство книг по информационной безопасности никогда не приносили своим авторам больше $10 000. Так было не всегда, но это остается фактом с тех пор, как стали популярны поисковые системы, с помощью которых можно бесплатно находить информацию. Существуют исключения. Я знаю несколько авторов книг на компьютерную тематику, которые заработали сотни тысяч долларов, и могут позволить себе яхты и дома на берегу. Но ни в коем случае не стоит писать книгу с целью разбогатеть. Это нужно делать для того, чтобы поделиться интересной идеей, которая может позволить десяткам тысяч читателей действительно улучшить свою жизнь или карьеру, или сделать что-то большее.

Хотя, обычно, авторы книг на компьютерную тематику не получают больших денег за книги, они, практически всегда, могут получить хорошо оплачиваемую работу. Будучи автором книги, вы зарабатываете доверие, практически, такое же, которое дает вам диплом или сертификат, но во многих случаях, уровень получаемого доверия даже выше. В среднем, авторы книг на компьютерную тематику, которых я знаю, зарабатывают гораздо больше тех, кто не писал книг. И повторюсь, за несколько часов я могу заработать больше, чем другие зарабатывают за неделю или две. И это говорит человек, который дважды провалил экзамен по письму.

Издаваться Самому или в Издательском Доме?

Если вы собираетесь написать книгу, вам нужно решить, хотите ли вы издаваться самостоятельно или работать с издательским домом. Для работы с издателем вам понадобится пройти процесс детального отбора. Для авторов, которые написали свою первую книгу может быть нелегко получить контракт, с гарантированными и постоянными выплатами гонорара. Многие авторы, те кто пишет впервые и не только, хотят издаваться самостоятельно, отчасти из-за того, что хотят получать больше прибыли за каждую проданную книгу. Но чаще всего авторы решают издаваться самостоятельно, так как получили отказ в издательском доме. Но это нелегкая задача (издаваться самостоятельно).

Если автор может гарантированно получать больший процент за каждую проданную книгу, не сотрудничая с издательским домом, то я уверен, что многим читателям будет интересно, зачем вообще с ним сотрудничать. Ну, есть множество причин. В среднем автор тратит, примерно, год на написание книги, кто-то больше, кто-то меньше. Если ему не повезло зарабатывать только писательской деятельностью, это означает, что он должен тратить на это все свое свободное время на протяжении года. В итоге, он не общается с семьей, пропускает вечеринки, и в целом, проводит за компьютером гораздо больше времени, чем он проводит, будучи специалистом по информационной безопасности. Учитывая все затраченные усилия, хочется, чтобы книга получилась хорошей. А книга, которая будет напечатана в издательском доме, скорее всего, получится гораздо лучше. Книги, изданные самостоятельно, редко продаются тиражом более нескольких тысяч копий (особенно в области информационной безопасности), и, как правило, просто не выглядят так же профессионально, как те, которые были выпущены издательским домом.

Сам факт прохождения отбора в профессиональном издательском доме делает вас, ваш стиль написания и саму книгу лучше. Плюс, издательский дом возьмет на себя "не писательскую" работу, объем которой может быть солидным. Перед написанием этой книги я задумался, стоит ли впервые попробовать издаваться самому, но потом я понял, что, если напишу главы и передам их издателю, который займется редактированием, техническими правками, шрифтами, маркетингом и распространением, и собственно, профессиональным созданием конечного продукта, то сэкономлю гораздо больше времени, которое смогу провести с семьей, или занимаясь другими любимыми делами, помимо писательской деятельности и информационной безопасности. Например, вместо того, чтобы самому создавать переднюю и заднюю обложки книги с нуля, я получил несколько макетов от редактора, и все они выполнены более креативно и более профессионально, чем те, что сделал бы я. Я просто выбрал те, которые мне понравились, и отправил ответ. Это заняло одну минуту, вместо нескольких дней или недель работы, а результат был лучше. Более того, качество работы профессиональных

редакторов из издательского дома, намного лучше работы ваших любимых или друзей, которые делают вам бесплатное одолжение.

Я думаю сотрудничество с издательским домом экономит, примерно, половину ваших усилий, и значительно увеличивает вероятность создания качественного продукта, который будет лучше продаваться, по сравнению с самостоятельным издательством. Таким образом, если вы преданный профессионал своего дела, и не боитесь вложить дополнительные усилия, то самостоятельное издательство - это реальная альтернатива. К сожалению, в мире тех, кто издается самостоятельно, полно некачественных работ с большим количеством опечаток. Это не означает, что в книгах, которые выпускают издательские дома, нет ошибок, но в целом, их гораздо меньше.

Если вы хотите отнести свою книгу в профессиональный издательский дом, зайдите на их веб-сайт и найдите раздел "предложить книгу". Не спешите его заполнять. Обычно на это уходит несколько дней. Затем отправьте предложение на их электронный адрес "для заказов" или человеку, который занимается такими вопросами. Если это ваша первая книга, и вы хотите, чтобы ее быстрее приняли, свяжитесь с литературным агентом, который занимается интересующей вас тематикой. Он поможет улучшить вашу идею и книгу. Мой опыт показывает, что результат почти всегда гарантирует получение контракта. Я не всегда пользовался услугами литературных агентов (я работал с StudioB (http://www.studiob.com/)), но когда я к ним обращался, их работа действительно стоила небольшого процента от моего гонорара с продажи книг (или других работ).

Технический Редактор

Задолго до того, как я стал публикуемым автором книг, я был техническим редактором, проверяющим книги, перед изданием. Я до сих пор им остаюсь. Многие авторы по информационной безопасности начинают с этого. Это отличная возможность понять, как все работает, чего ждут от автора, и как избежать ошибок, которые свойственны начинающим авторам.

Новостные Рассылки

Существуют десятки ежедневных, еженедельных и ежемесячных новостных рассылок по информационной безопасности, для которых вы можете писать. Понадобится приложить усилия, чтобы стать автором признанных журналов и новостных рассылок, которые уже давно существуют. Многие из них вообще не принимают новых, добровольных публикаций от авторов, в то время, как другие, менее известные новостные рассылки, безумно сильно нуждаются в новых авторах. Новостные рассылки - это отличное место, где можно выработать свой стиль письма и работа в них будет отличной строчкой в

резюме, которая позволит в дальнейшем получить другую, высокооплачиваемую работу.

Брошюры

Мой опыт показывает, что, во многих случаях, брошюры, спонсируемые производителем - это легкий способ заработать большие деньги. Производители всегда предлагают высокую оплату за брошюру длиной в 5 - 10 страниц. Некоторые темы давались мне легко, и я писал всю брошюру в течение нескольких часов. Другие темы требовали больше исследований и интервью, и работа могла занимать многие недели. Но, в целом, за несколько брошюр можно заработать такие же деньги, как за книгу, затратив намного меньше усилий. Проблема в том, что во многих случаях, написать брошюру просят именно автора книги. Тем не менее, следует помнить, что с точки зрения этики, если производитель хотя бы раз платил вам за выполнение работы по продвижению, то вы всегда должны указывать на это во всех работах, которые вы пишите для того же производителя или его конкурентов.

Технические Обзоры

Самая сложная писательская работа, которой я когда-либо занимался - это написание технических обзоров. Они подразумевают проверку одного или несколько продуктов, оценку того, настолько ли они хороши, как об этом постоянно говорят производители. После чего нужно сообщить читателям о настоящих возможностях этих продуктов. Такие обзоры могут занимать несколько дней или недель, и часто требуют применения лабораторных тестов, а также интервью с реальными пользователями. И за все эти усилия, производители, как правило, платят меньше, чем за брошюры, которые гораздо легче написать. Учитывая все вышесказанное, хороший технический обзор может принести гораздо больше удовлетворения от работы, и помочь большему количеству людей. Каждый год я пытаюсь делать несколько таких обзоров. Я делаю обзоры, когда вижу многообещающий продукт или если продукт интересен читателям.

Конференции

Как только вы станете профессиональным писателем, вас, возможно, начнут приглашать на конференции, на которых вы можете выступить с презентацией. Мне понадобилось два десятилетия, чтобы справиться со страхом сцены, пробирающим до дрожи в коленях, но я с уверенностью могу сказать, что выступления на конференциях приносят огромное удовольствие от проделанной работы. Это не только дает возможность поделиться полученными

знаниями, выступая с интересной вам темой, но и встретить десятки единомышленников, получить новые возможности для продвижения по работе, и открыть для себя факты, которых вы раньше не знали. Конечно, выступление с презентацией требует определенных навыков, таких, как создание качественных слайд-шоу и проработка грамотного стиля ведения презентации. На многих конференциях есть предварительные тренинги, которые призваны помочь новым (и опытным) участникам улучшить свои ораторские навыки и навыки презентации.

Советы Профессионального Писателя

После, практически, трех десятилетий писательской деятельности, я могу дать своим читателям несколько советов, в том числе те, что описаны ниже.

Сложнее Всего Начать

За годы работы, ко мне подходили сотни людей, с вопросом, как стать профессиональным писателем. Я всегда даю им много информации и рекомендаций. И за все это время, наверное, только некоторые из них последовали моим советам и хотя бы попытались. Быть профессиональным писателем в технической области не просто, по крайней мере, без достаточной практики. Самое сложное - начать. Если вы хотите профессионально писать, частично или полностью уделяя этому свое время, вам нужно начать писать и прикладывать все возможные усилия, чтобы вас опубликовали. Конечно, вы должны разбираться в своем предмете, и уметь хорошо писать, но, как я уже говорил, что-то из этого можно выучить в процессе. Если у вас не получается понятно и интересно писать, прочитайте несколько книг по грамматике и искусству написания текстов.

Читайте По-другому

Также, как и профессиональный музыкант, который слушает музыку не как обычный поклонник, писатель должен оценивать тексты других. Ему необходимо видеть в тексте идеи, подсказки и различные приемы. Начните читать статьи, старайтесь разглядеть в них авторские приемы. Как автор знакомит читателя с историей? Каким было первое предложение? Насколько хорошо раскрыт материал? Было ли интересно? Использовал ли автор графику, и где? Каким был вывод? Если вы собираетесь стать профессиональным писателем, вы должны замечать кирпичики в фундаменте дома. Кроме того, если вам понравился стиль какого-то автора, прочтите другие его произведения. Как только вы найдете такого автора и будете читать его тексты

из-за того, что они написаны лучше, чем большинство произведений других авторов, продолжайте изучать его материалы.

Начните Писать Бесплатно

Очень редко авторы получают деньги за свою первую работу. Многим из нас пришлось потратить свое время, чтобы, скажем так, попасть на передовую. Если вы хотите начать карьеру профессионального писателя, ищите наиболее известные новостные рассылки и блоги, которые принимают бесплатные статьи и идеи, и продолжайте делать шаги в этом направлении. Со временем, набирая опыт, и создавая собственный стиль письма, вы сможете начать повышать запросы, тем не менее, следует помнить, что разные виды писательской работы оплачиваются по-разному. Целью такой работы не всегда должны быть деньги. Каждой новой публикацией вы зарабатываете репутацию.

Будьте Профессиональны

В конце концов, само собой разумеется, что в индустрии профессиональных авторов, нужно быть профессиональным во всем. Это означает, что нужно быть подготовленным и обладать соответствующими знаниями, но также - не проваливать дедлайны. Каждый редактор и издатель в этой индустрии может рассказать вам историю ужасов, о том, как они подписали с автором контракт, а он так и не закончил книгу или статью. Я узнал, что если просто сдавать все в срок, то можно взять работу и получить много денег. Во многих случаях, когда вы первый раз встречаетесь с издателем или редактором, он пытается понять насколько вы надежны и профессиональны. Если от раза к разу демонстрировать профессионализм, то можно стать профессиональным писателем. Если у вас получается это делать на протяжении длительного времени, значит получится и на протяжении всей карьеры.

Станьте Своим Рекламным Агентом

Независимо от того, хотите ли вы издаваться самостоятельно или использовать услуги профессиональной организации, вам нужно сделать все возможное, чтобы вашу работу увидело, как можно больше людей. Вот почему у многих профессиональных авторов по информационной безопасности есть профили в различных социальных сетях. Чем больше людей о вас знает, тем выше шанс, что вы сможете зарабатывать писательской деятельностью.

Картина, Которая Стоит Тысячи Слов

Я выражаю благодарность моему давнему другу и профессиональному автору бестселлеров в IT-сфере Марку Минаси (http://www.minasi.com), за этот совет: «Чтобы бы ты не писал, всегда добавляй свою фотографию в профиль. Читателям будет намного легче запомнить вас, если у них будет возможность ассоциировать изображение с вашим именем. Поначалу, я говорил администрации веб-сайтов, что буду писать бесплатно (даже, если они предлагали заплатить), если у меня будет возможность разместить рядом со статьей свое фото. Это позволяет быстрее создать узнаваемость имени и набрать последователей, что является залогом успеха. Существует побочный эффект, способствующий росту вашего эго - иногда, к вам подходят совершенно незнакомые люди, и говорят, что им нравится ваша работа. Мои книги никогда не оказывали сильного впечатления на моих дочерей, но в ресторане или в парке аттракционов ко мне подходили случайные поклонники, которые узнавали меня и выражали благодарность.

Так как моя основная работа - консультант по информационной безопасности, я не только писатель, но писательская деятельность определенно оказала положительный эффект на мою работу консультанта. Когда вы пишите, вы должны очень хорошо разбираться в предмете, знать его, практически, в совершенстве. Это вынуждает настолько много учиться и тренировать свой мозг, что я бы не делал этого, не будь я автором книг. Мне нравится думать, что работа консультанта по информационной безопасности делает меня лучше, как писателя, а работа писателя делает меня лучше, как консультанта по информационной безопасности. По крайней мере, в моем случае, одна работа не совпадает с другой.

В следующей главе мы поговорим о Фамиде Рашид, ведущим авторе и моей коллеге в журнале *InfoWorld*.

Глава 48. Профиль: Фамида Рашид

Я работаю техническим журналистом в сфере информационной безопасности почти 30 лет. Хотя я не лучший писатель, я считаю себя одним из лучших авторов технического материала, так как я живу и дышу своим предметом. Обычно, когда я читаю работы других авторов по информационной безопасности, я не изучаю что-то новое. Это изменилось, когда главный редактор журнала *InfoWorld*, Эрик Кнорр, представил мне нашего нового автора. Эрик был очень рад, когда нанял ее, и вскоре я узнал почему. Как и Брайан Кребс, журналист, занимающийся информационной безопасностью, Фамида Рашид - невероятный профессионал в вопросах исследования информационной безопасности, хотя и работает в другом направлении. Мне еще предстоит прочитать хотя бы одну статью за ее авторством, из которой я бы не узнал чего-то нового. Она настолько хорошо понимает свой предмет, что продолжает удивлять меня, словано я не являюсь специалистом по информационной безопасности. Она действительно хорошо разбирается в технических деталях, и умеет выискивать интересные темы лучше, чем кто-либо в этом деле. Иногда она чего-то не знает, и отправляет мне вопросы по технической части, на которые я, практически, всегда отвечаю "я тоже не знаю", но через несколько дней, проведя больше исследований, она публикует понятное объяснение. Она сама находит ответы.

Она опытный журналист в сфере информационной безопасности. Она работала в журнале eWeek в качестве старшего технического редактора подразделения CRN Test Center, она занималась сетевой инфраструктурой сайта Forbes.com, была главным редактором на мероприятиях RSA Conference, и писала для десятков уважаемых журналов и веб-сайтов, таких как: Dark Reading, PCMag.com, SecurityWeek, Tom's Guide, *InfoWorld*, SCMagazine, Dice.com, BankInfoSecurity.com и GovInfoSecurity.com. В данный момент она ведущий автор журнала *InfoWorld*, а также работает в Pragmatic Bookshelf, помогая авторам освоить процесс написания книг по технологиям.

Я спросил Рашид, как она начала работать в сфере информационной безопасности. Она ответила: "На самом деле, я начинала в качестве технического специалиста по сетям и специалиста техподдержки для студентов, преподавательского состава и администраторов в крупном университете. Я многое узнала о безопасности сетей, когда столкнулась с вызовами концепции BYOD. Это произошло задолго до того, как этот акроним стал популярен в сфере безопасности. У меня был печальный опыт изучения администрирования веб-серверов. Когда я была разработчиком ПО в

ColdFusion, кто-то взломал IIS-сервер и удалил все файлы. Шесть лет я работала консультантом по вопросам управления в различных финансовых и фармацевтических компаниях, разрабатывала приложения на Java, создавала огромные хранилища данных и управляла огромными массивами данных. Хотя мне и нравилась эта работа, я хотела сделать шаг назад и взглянуть шире на мир технологий. Я не хотела просто следить за сетью одной компании. Я стала работать журналистом, освещающим вопросы технологий и писала о сетях, хранилищах данных и "железе". Мне пригодились все мои технические знания, я действительно понимала, как работает технология, о которой я пишу.

Сфера безопасности стала логическим продолжением моей деятельности, потому что, на самом деле, сложно писать о сетях, и не думать о безопасности. Спустя, примерно, пять лет, я начала специализироваться на безопасности информации. Отчасти это была счастливая случайность, так как количество профессиональных атак, инсайдерских утечек и мошеннических операций с кредитными картами росло, мне пришлось больше времени уделять безопасности. Я стала разбираться в работе сетей, поэтому могла увидеть недоработки, которые делали атаку возможной. Я начала изучать SQL-инъекции и XSS-уязвимости, и искренне надеялась, что ни один из кодов, которые я писала, когда работала консультантом, больше не используется, потому я писала небезопасный код. Я писала, как для потребителей, так и для бизнеса, и поняла, что две эти группы, совершенно по-разному смотрят на безопасность. Но я рада видеть, что спустя все эти годы, люди все больше задумываются о безопасности, а не расценивают ее только, как работу технических специалистов".

Я спросил Рашид, что, по ее мнению, является главной проблемой информационной безопасности. Она ответила: "Я думаю, что главная проблема в сложности реализации безопасности. Это требует выработки новых привычек, а у нас нет на это ни времени, ни терпения. Этот процесс и не должен быть легким или удобным, но когда он сбивает с толку, польза от конечного результата уже не так очевидна, и люди просто начинают искать обходные варианты. Абсолютно все современные проблемы безопасности исходят из того факта, что работать, обеспечивая максимальную безопасность, сложнее, и намного проще оставить все открытым и незащищенным. Вот несколько примеров: шифрование действительно обеспечивает безопасность, но его все еще сложно использовать на постоянной основе. WhatsApp автоматически шифрует сообщения, так что теперь людям не нужно использовать секретные чаты. Но реализовать безопасную передачу файлов и зашифрованных электронных писем все еще тяжело.

Мы не думаем дважды, когда запираем двери наших домов, но наверняка были времена, когда люди считали это безумием. И в данный момент, мы находимся на стадии, когда люди думают, что соблюдать все шаги для обеспечения безопасности - безумие, но это мировоззрение медленно

меняется. Но, чтобы оно действительно изменилось, нам нужны инструменты получше. С другой стороны, я знаю очень много людей, которые все еще не используют TouchID на смартфонах Apple, и я не знаю, насколько еще более "не сложными" должны быть способы защиты информации, чтобы люди о ней задумались. Возможно их телефоны должны автоматически сохранять отпечатки пальцев пользователей, без ручной настройки TouchID. Нам нужна безопасность по умолчанию, чтобы двери закрывались автоматически, без необходимости вытаскивать ключ. Skynet может быть решением всех наших проблем, связанных с безопасностью".

Я спросил Рашид, которая долгое время успешно работает журналистом, освещая проблемы информационной безопасности, что она может посоветовать тем, кто рассматривает карьеру писателя в сфере информационной безопасности. Она сказала: "Хотя я не думаю, что для начала карьеры писателя, вам нужны технические знания, но их наличие сильно помогает. Я не говорю, что нужно получать сертификат CISSP, писать код или научиться использовать Metasploit. Но нужно знать основы работы сетей, как взаимодействуют компьютеры и другие устройства, и значение основных терминов. Если вы собираетесь говорить об атаках на веб-приложения, нужно понимать схему взаимодействия веб-приложений, веб-серверов и баз данных. Если вы собираетесь писать о DDoS-атаках (или их младших собратьях DoS-атаках), у вас должно быть базовое представление о работе сетей. Не обязательно понимать, как именно устроены алгоритмы шифрования, но необходимо понимать разницу между различными алгоритмами, и почему некоторые из них не стоит использовать. Читайте. Изучайте технологии. Не бойтесь понять, как работает технология. Нельзя объяснить людям, что нужно лучше защищать нашу цифровую жизнь и технику, если вы сами боитесь технологий. Думайте об этом в таком ключе - не нужно быть пилотом самолета, чтобы писать об индустрии авиации, но, если бы вы летали хотя бы на нескольких самолетах, то это бы сильно помогло.

Другой важный момент, который нужно помнить - как правило, технологии используются волнообразно. Новое - это хорошо забытое старое, но с некоторыми доработками. Количество молодых писателей, которые не знают о мейнфреймах или махают на них рукой, потому что "их больше никто не использует", пугает, потому что мейнфреймы являются основой многих современных устройств. Снова возвращается управление правами доступа к данным. И каждый раз, когда я слышу, как люди говорят о мобильных устройствах или данных в облаке, я вспоминаю о временах, когда только появлялся тонкий клиент. Всегда важно знать прошлое, особенно, в случае с безопасностью, так у вас будут примеры".

Я спросил ее о знаниях, которые могли бы помочь ее карьере. Она ответила: "Не бойтесь задавать вопросы. Я думала, что эксперты и исследователи безопасности будут относится ко мне серьезно, если я уже буду хорошо знать

основы, поэтому я потратила огромное количество времени на изучение основ. Мне понадобилось очень много времени, чтобы понять, что эксперты хотят, чтобы им задавали вопросы. Это их возможность похвастаться своими знаниями. Но нужно знать основы - не спрашивайте их о том, что такое DDoS-атака, но вы можете попросить объяснить подробности, например, в чем разница, между DoS-атакой на 4 и 7 уровнях. Многие основы безопасности я изучала самостоятельно, и, если бы я попросила помощи раньше, я бы могла детальнее разобраться в вопросе (а не зубрить), и не испытывать и половины стресса, который был во время самостоятельного обучения. Также, относитесь скептически к таким словам, как "инновационный", "самый первый" и "лидер рынка". На самом деле, когда вы видите анонсы в сфере безопасности, вычеркните из них громкие слова. Так вы сможете увидеть суть сообщения".

Я спросил Рашид, почему ей нравится писать статьи на тему информационной безопасности. Она ответила: "Мне нравится область информационной безопасности, потому что я постоянно должна учиться. Всегда можно почитать новое исследование, и всегда можно узнать новые способы решения проблем. Безопасность совмещает решение проблем, любопытство и желание что-нибудь сломать, для того, чтобы что-то улучшить. Эта область также работает на эго. Профессионалы по безопасности - люди, которые каждое утро просыпаются с желанием спасти мир, все данные и устройства одновременно. Возможно у них нет миллионов, которые зарабатывают создатели Instagram, или славы Илона Маска, но люди, которые обеспечивают безопасность моих данных в базах корпораций, следят за тем, чтобы SSL-сертификат веб-страницы был актуален, чтобы мои финансовые данные были безопасно переданы по интернету, и тестируют код ПО, чтобы обеспечить в нем отсутствие уязвимости, с помощью которой возможно удаленно выполнить код - это те, кто спасает для нас мир. Мне нравится писать об информационной безопасности, потому что так я становлюсь ближе к этим героям".

Подробнее о Фамиде Рашид

Подробнее о Фамиде Рашид вы можете найти на этих ресурсах:

- Профиль Фамиды Рашид в LinkedIn: https://www.linkedin.com/in/fyrashid
- Статьи Фамиды Рашид в журнале *InfoWorld*: http://www.infoworld.com/author/Fahmida-Y.-Rashid/

Глава 49. Пособие для Родителей Молодых Хакеров

ПРИМЕЧАНИЕ Часть этой главы взята из статьи, которую я написал в 2016-ом: “11 признаков того, что ваш ребенок хакер, и что с этим делать” (http://www.infoworld.com/article/3088970/security/11-signs-your-kid-ishacking-and-what-to-do-about-it.html).

Будучи автором статей о информационной безопасности более 20 лет, несколько раз в год я получаю электронные письма от родителей, которые спрашивают меня, как определить, что их ребенок становится хакером - плохим хакером - и что они могут сделать, чтобы воодушевить его начать многообещающую, честную карьеру. Я понимаю, о чем они говорят, потому что много лет назад у меня была та же ситуация с моим сыном. Он начал заниматься “не таким уж законным” взломом, иногда, у него были небольшие неприятности. К счастью, мы с женой рано вмешались, и, не без труда, помогли ему стать хакером в белой шляпе.

Я думаю, многие умные подростки, интересующиеся компьютерами, могут стать хакерами в черных шляпах, если не дать им правильного наставления. Часто они либо не очень хорошо учится в школе, либо не получают большого удовольствия от школьных достижений. В школе и, вероятно, дома, им говорят, что нужно делать то, что они считают скучным и бессмысленным, и они думают, что это наказание за то, что они не раскрывают свой потенциал. В онлайн-мире они могут получить одобрение и уважение своих единомышленников. Они чувствуют себя сильными и, в то же время, загадочными. Это похоже на наркотик. Я понимаю эту тягу. Большинство из этих детей - хорошие ребята, и они забросят хобби хакера в черной шляпе, не попадая в неприятности. Проблема в том, что нельзя быть уверенным, что ваш ребенок точно бросит это увлечение, поэтому лучше всего вмешаться до того, как ему придется понять, как сложно найти работу, имея судимость.

Признаки Того, Что Ваш Ребенок Хакер

Перед тем, как советовать своему ребенку использовать его хакерские навыки только в благих целях, вы должны точно узнать, что его деятельность наносит вред. После того, как вы выяснили, что их секретность не связана только с

порнографией или девушкой, или парнем, вы можете обнаружить несколько признаков, которые указывают на то, что ваш ребенок - хакер. Следующие разделы описывают эти признаки.

ПРИМЕЧАНИЕ Существует много вопросов, которые могут беспокоить родителей, когда их ребенок "сидит" в интернете, например, просмотр порнографии, общение в чатах с преступниками, и другие виды активности, которые могут быть опасными или привести к проблемам с законом. Каждый из этих вопросов требует рассмотрения, и может быть решен различными способами, но в этой главе, мы будем говорить именно об опасности, которую может повлечь хакерская деятельность.

Они Сами Говорят Вам, Что Взламывают

Это самый простой вариант. Ваш ребенок рассказывает или хвастается вам, как легко можно что-то взломать. Я знаю, это звучит забавно, но некоторые родители слышат такие откровенные заявления, часто по многу раз, и игнорируют их. Они либо не понимают, про какое "хакерство" говорит их ребенок, либо думают, что их ребенок, который всегда был хорошим, не сделает чего-то плохого или глупого. К сожалению, иногда именно так и происходит.

Слишком Активно Скрывают Свою Деятельность в Интернете

Каждый подросток хочет 100% конфиденциальности всех свои действий, в интернете и не только, независимо от того, является ли он хакером. Ребенок-хакер идет еще дальше и скрывает все свои действия. Я говорю о полном удалении результатов их деятельности в сети. Их история в браузере всегда пустая. Логи "чистые". Нет новых файлов или папок. Все спрятано. Отсутствие любой активности - большой признак того, что они намеренно скрывают деятельность, из-за которой у них могут быть большие неприятности. Кстати, чистить историю в браузере они могут и по другим причинам, поэтому я говорю не только об этом.

У Них Есть Несколько Email-аккаунтов/Аккаунтов в Социальных Сетях, к Которым Вы не Можете Получить Доступ

Это нормально, если у ребенка есть несколько Email-аккаунтов и аккаунтов в социальных сетях. В данном случае, проблема в том, что к ним нельзя получить

доступ. Если у вашего ребенка есть электронная почта или аккаунт в социальной сети, которые он может спокойно вам показать, и вы узнаете, что у него есть и другие аккаунты, с другими учетными данными, которые он от вас прячет, значит что-то не так.

Вы Нашли на Компьютере Инструмент для Взлома

Если вы нашли инструменты для взлома, описанные в этой книге или те, которые обычно есть на хакерских сайтах, то скорее всего, ваш ребенок интересуется взломом.

Вам Говорят, Что Вы Взламываете

За тот период, пока мой сын интересовался хакерством, мне несколько раз поступали электронные письма или звонки от незнакомых людей или моего интернет-провайдера с предупреждениями, что если я продолжу хакерскую деятельность, то мне отключат интернет или даже подадут в суд, и я буду вынужден отвечать по закону. Поначалу я ничего не понимал. Я никого не взламывал. Это делал мой сын.

Они Сворачивают Приложение Каждый Раз, Когда Вы Заходите в Комнату

Есть много того, что они хотят спрятать, сворачивая приложение, когда вы заходите в комнату (например, порнографию или общение с девушкой/парнем), но, если они делают это каждый раз, когда вы заходите в комнату, узнайте почему они так делают.

Все Эти Признаки Могут Относится и к Обычным Подросткам

Все это может быть свойственно и обычным подросткам. Ваш ребенок может и не быть хакером. Я уверен, многие читатели и их дети прямо сейчас читают эту главу и говорят, что с ними происходило все из вышеперечисленного и они никак не были связаны с незаконным или неэтичным хакерством. Я понимаю. Я просто хочу рассказать о признаках, которые могут указывать на то, что ваш ребенок хакер, чтобы вас не застали врасплох, как застали меня, мою жену и многих читателей, которые мне пишут.

Хакерство - Это Не Всегда Плохо

На самом деле, в основном, это хорошо. Хакер - это тот, кто просто хочет выйти за рамки стандартного GUI или другого интерфейса, который есть у обычного пользователя. Я хакер, и за всю свою жизнь я не совершал ничего противозаконного. Это также относится и ко многим моим коллегам (хотя некоторые какое-то время были на темной стороне, когда были моложе). Если вы думаете, что ваш ребенок занимается взломом, то перед тем, как отнимать у него компьютер, вы должны выяснить, являются ли его действия неэтичными или незаконными. Как правило, у руководителей и сотрудников самых влиятельных компаний есть хакерская этика. Остается лишь убедиться, что определенная хакерская деятельность является этичной и законной.

Как Исправить Своего Юного Хакера

Итак, предположим, вы узнали, что ваш ребенок занимается неэтичным или незаконным взломом. Что можно сделать?

Во-первых, нужно понимать, что ребенка можно направить в верное русло. Большинство из детей перестает заниматься незаконной деятельностью, когда они взрослеют и находят себя в другой работе, которая лучше оплачивается и не является нелегальной. Лишь некоторые продолжают карьеру хакера в черной шляпе. Суть в том, чтобы направить таких детей, которые знают, что поступают нехорошо, и использовать их недавно обнаруженные навыки во благо.

Во-вторых, дайте им понять, что вы знаете о происходящем, и что их действия неэтичны, незаконны и могут привести к их аресту. Времена, когда компании и власти ничего не знали и редко кого-то арестовывали, давно прошли. Хакеров постоянно арестовывают и заводят на них дела. У меня есть талантливые, компетентные коллеги с судимостью, которая до сих пор не дает им составить мне компанию на определенных высоких должностях.

В-третьих, скажите своим детям, что вы будете наблюдать за их деятельностью столько, сколько понадобится. Дайте им понять, что вы будете наблюдать за ними, но не раскроете подробностей о том, что именно вы будете делать. И предупредите их, что если вы заметите хотя бы малейшие проявления неэтичной или нелегальной активности, они надолго попрощаются со всеми гаджетами, которые у них есть. Пригрозите запретом любой деятельности, которая им нравится. Нужно их немного припугнуть, и дать понять, что будут последствия. Если они нарушат эти правила, приводите угрозы в исполнение.

Перенесите Их Компьютер в Основную Жилую Комнату и Наблюдайте

Если компьютер вашего ребенка стоит в его комнате, лишите его этих привилегий, и перенесите компьютер в основную жилую комнату, чтобы вам было легче за ним следить. Запретите ему пользоваться компьютером, когда вас нет дома, и вы не можете наблюдать. Скажите, что такие изменения будут работать до тех пор, пока вы не сможете снова ему доверять. Продолжайте следить за действиями вашего ребенка, даже когда он сидит перед вами.

Дайте Наставления

Помимо лишений и потенциальных наказаний, ребенку нужно давать наставления. Поговорите с ним о важности этики, как в интернете, так и в обычной жизни. Объясните, что любая хакерская деятельность без соответствующего разрешения, выданного законным владельцем или организацией, в которой хранятся данные, является незаконной. Объясните ему, что даже неочевидная хакерская деятельность, такая как использование открытого порта или сканирование на наличие уязвимостей, может быть незаконной, но даже если она является законной, это все равно неэтично.

Расскажите Им о Местах, Где Можно Законно Взламывать

Если ваш ребенок интересуется взломом, расскажите ему о местах, где можно заниматься законной и этичной хакерской деятельностью, в которых он может выражать свою креативность и учиться. Существует множество таких мест.

Веб-сайты HackMe (Взломай Меня)

В интернете существует множество различных веб-сайтов, которые созданы специально для того, чтобы их взламывали. Поищите такие сайты. Один из моих любимых - Hack This Site (https://www.hackthissite.org/). Этот сайт можно взламывать, и он объединяет десятки групп и проектов, посвященных взлому. Еще один сайт, посвященный различным хакерам, не только тем, которые взламывают компьютеры - Hacker Spaces (http://hackerspaces.org/wiki/).

Программы Поощрения Поиска Багов

У многих производителей есть программы поощрения за обнаружение багов, они выплачивают деньги за их обнаружение. Некоторые производители платят сотни тысяч долларов за обнаружение критических багов, и уже выплатили по таким программам миллионы долларов. Многие молодые люди заработали

тысячи долларов, сообщая о багах, включая вот этот случай (https://www.pcmag.com/article2/0,2817,2371391,00.asp&title=12-Year-Old%20Earns%20$3,000%20Bug%20Bounty%20From%20Mozilla). Такие программы есть у многих известных производителей:

- Программа Microsoft: https://technet.microsoft.com/en-us/library/dn425036.aspx.
- Программа Google: https://www.google.com/about/appsecurity/reward-program/.
- У Apple такая программа работает только по приглашению, но они тоже платят посторонним пользователям за сообщения о багах.
- Программа Mozilla: https://www.mozilla.org/en-US/security/bug-bounty/.
- HackerOne (https://www.hackerone.com) - компания, которая координирует программы поощрения других компаний, таких как Twitter, Slack и Airbnb.

Не у каждого производителя есть программа поощрения за обнаружение багов, но у всех умных - она есть.

Взлом Аппаратных Компонентов

Если вашему ребенку интереснее взламывать аппаратные, а не программные компоненты, то существует множество вариантов выхода в такой ситуации. Он может присоединиться к хакерским группам, взламывающим IoT-устройства, о которых мы говорили в Главе 35. В них он может узнать, как взламывать настоящие IoT-устройства, либо он может начать с основ взлома аппаратных компонентов, используя набор Raspberry Pi (https://www.raspberrypi.org/). Raspberry Pi - это, по сути, крохотный одноплатный компьютер, который работает под управлением линукс. Было продано уже более 10 миллионов экземпляров. Еще один схожий продукт - Arduino (https://www.arduino.cc/). Времена, когда все, что можно было сделать - купить схемы, провода, чипы и изучать, как можно что-то из этого спаять, давно прошли. С нынешними устройствами, вы и ваш ребенок, сможете реализовать миллионы DIY проектов.

Клубы Робототехники

Поищите местные клубы робототехники. Многие учебные заведения и компьютерные производители спонсируют клубы робототехники, которые особенно заинтересованы в молодых хакерах, а ведущие учебные заведения и производители обеспечивают высочайший уровень таких клубов. Если вы не можете найти местный клуб, то RoboRealm

(http://www.roborealm.com/clubs/list.php) и Arrick Robotics (http://arrickrobotics.com/clubs.html) это отличные ресурсы с которых можно начать.

ПРИМЕЧАНИЕ Еще одно хобби, которое может быть интересно начинающим хакерам - любительская радиосвязь. Многие мои друзья-хакеры также давно увлекаются любительской радиосвязью. Должно быть, в этом есть какая-то интеллектуальная связь.

Соревнования Capture the Flag

Многие учебные заведения, веб-сайты, группы и конференции по безопасности спонсируют соревнования "capture the flag" (захват флага), где хакеры или команды хакеров состязаются в скорости взлома ради получения приза. Просто наберите в любом поисковике "соревнования capture the flag", и вы увидите десятки таких соревнований, в которых вы или ваш ребенок можете принять участие. Есть сайт, на котором указаны многие предстоящие соревнования capture the flag: https://ctftime.org/.

Обучение и Сертификаты

Обучение или прохождение сертификации - это отличный способ направить юный хакерский пыл в правильное русло. Бросьте вашему ребенку вызов, чтобы он смог получить сертификат по информационной безопасности (некоторые из которых описаны в Главе 41), и тем самым, показать, насколько он хорош. Получая первый сертификат, который признан повсеместно, например, сертификат EC-Council Certified Ethical Hacker (Сертифицированный этичный хакер, CEH), он сможет многому научиться и серьезно продвинуться в карьере. За практически 30 лет хакерской деятельности, я узнавал что-то новое и важное, получая каждый сертификат, и значительно улучшил свои хакерские навыки.

Дайте Им Хорошего Наставника

Наконец, попытайтесь познакомить их с человеком, который пережил тот же опыт, и смог направить свои креативные навыки на построение законной и прибыльной карьеры. Если вы не знаете таких людей, то я готов помочь (roger_grimes@infoworld.com). Я с радостью добавлю вашего ребенка в список своих учеников.

Как правило, я даю те же наставления, которые изложены в этой книге, но я также могу познакомить их с другими умными, хорошими хакерами. Многие дети ошибочно считают, что хакеры в черных шляпах самые умные и сообразительные. Но каждый год, возможно, один плохой хакер делает что-то

новое и интересное. Все остальные просто повторяют действия других. Без сомнений, лучшие хакеры, которые я встречал - это защитники.

Легко взять кувалду и разнести автомобиль, но гораздо сложнее создать этот автомобиль. Хотите произвести на меня впечатление? Попробуйте создать что-то, что сможет выдержать постоянные атаки хакеров.

Если вы подозреваете, что ваш или чей-то еще ребенок занимается неэтичным или незаконным взломом, покажите ему эту книгу. Подростков, которые любят взламывать, всегда можно "обратить" на светлую сторону. И если на то пошло, то взрослых тоже.

Что насчет моего сына? У него отличная жизнь. У него отличная работа, связанная с компьютерами, которая приносит хороший доход, он отличный сын, отец, и этичный человек. Я очень его люблю. Мы со смехом вспоминаем времена, когда мы "сражались" с ним в цифровом мире. Он благодарен мне и своей маме за то, что мы вмешались и дали наставления, которые помогли ему уйти с темной стороны хакерства.

Глава 50. Кодекс Этики Хакера

Если вы поищите в интернете "хакерскую этику", то, скорее всего, найдете приукрашенную версию так называемых "хакерских правил", которые объединены в идею, что для достижения любой своей цели, хакеры могут делать все, что захотят, возможно даже без всяких ограничений. Бестселлер Стивена Леви *Hackers: Heroes of the Computer Revolution* (https://www.amazon.com/Hackers-Computer-Revolution-Steven-Levy/dp/1449388396/) представил миру одну из первых версий хакерской этики (https://en.wikipedia.org/wiki/Hacker_ethic). Если вкратце, то, практически, слово в слово там написано следующее:

1. Доступ к компьютерам должен быть неограниченным для каждого.
2. Вся информация должна быть свободной.
3. Недоверие властям и продвижение принципа децентрализации.
4. Оценивать хакера можно только за его достижения. Ни положение в обществе, ни возраст, ни раса не играют при этом никакой роли.
5. С помощью компьютера каждый может создавать произведения искусства.
6. Компьютеры могут изменить жизнь к лучшему

Леви показывал, но не всегда соглашался с тем, что в те дни думали многие хакеры. К сожалению, многие хакеры восприняли хакерскую этику Леви, как утверждение, что цель оправдывает средства, и что даже незаконная деятельность - это не плохо. Это все равно, что утверждать, что грабить банки или красть чью-то собственность - это хорошо, если тем самым вы помогаете бедным. Действия хакеров, не имеющих моральных принципов, могут быть неэтичными, и приводить к проблемам с законом. Но самое ужасное то, что такие действия вредят всем нам.

Даже исключив тот момент, что книга Леви была написана за десять лет до бурного развития информационных технологий, он не призывал заниматься незаконной и неэтичной деятельностью. Несмотря на то, что действия некоторых людей, описанных в его книге, были спорными с точки зрения этики, большинство действовало этично. Многие улучшили свою жизнь и жизнь общества, не сделав ничего противозаконного. Многие самозабвенно посвятили всю свою жизнь улучшению жизни других людей, и не получили за это, практически, никакого денежного вознаграждения. Хотя некоторые хакеры увидели в хакерской этике Леви свободу для всех и возможность не соблюдать

закон. Как еще понимать фразу "Вся информация должна быть свободной"? Большинство читателей и начинающих хакеров увидели красоту работы при соблюдении этических норм. В книге Леви хакеры, поначалу, могли быть децентрализованными, не доверяющими властям, свободными мыслителями, но в конце концов, полученные ими знания, их творения и изобретения изменили весь мир к лучшему.

Если бы вся информация действительно находилась в свободном доступе, то у лучших в мире художников и писателей пропал бы стимул создавать свои удивительные произведения. Даже Стивен Леви хотел, чтобы ему заплатили за эту книгу. Большинство производителей аппаратных компонентов и программистов не смогли бы делать то, что делают, если бы это не приносило определенного дохода. В конце концов, кто-то должен платить за работу, которая выстраивает шоссе для информационных технологий. Если бы создатели и владельцы не получали денег за свои продукты и информацию, то у нас бы было намного меньше и продуктов, и информации. Если бы использовали только самые основы хакерской этики, исключив моральную составляющую, то у нас бы не было такого замечательного общества. Именно, взлом ради высшей цели, исключающий морально-этические нормы, просто сделал бы общество более порочным.

Кульминационный момент книги заключается в демонстрации того, что лучший взлом - это этичный и легальный взлом. Все, кто представлен в его книге использовали свой невероятный интеллектуальный дар во благо человечества.

Основной посыл книги в том, что хакерская деятельность не должна наносить миру больше вреда, даже, если это может принести славу и удачу. Мораль должна быть важнее денег и славы. Это не значит, что деньги и слава - это плохо, но их нужно зарабатывать, соблюдая закон и этические нормы.

Сегодня во многих организациях, занимающихся подготовкой специалистов по информационной безопасности, есть кодекс этических норм, который нужно соблюдать. Без этого невозможно получить их сертификат. Самый популярный кодекс хакера, который я нашел в интернете - это кодекс этики EC-Council (https://www.eccouncil.org/code-of-ethics/). Это хороший кодекс, но он слишком сильно фокусируется на тестировании на проникновение, и со временем становится длиннее (на момент написания этой книги в нем было 19 пунктов). Учитывая все вышесказанное, в следующем разделе описан хороший, краткий кодекс этики, который я составил, опираясь как на личный, так и на профессиональный опыт.

Это мой собственный кодекс этики, на который я опираюсь всю свою жизнь. И я думаю, что он отлично подходит любому хакеру

Будьте Открытыми, Честными и Соблюдайте Этические Нормы

Не нужно говорить, что соблюдение кодекса этики означает соблюдение моральных норм. Их соблюдение означает выбор только в пользу правильных поступков, добра, а не зла, правосудия, а не несправедливости. Если у вас есть моральный выбор, то его нужно делать в пользу блага для общества. Работайте открыто, чтобы заинтересованные стороны могли видеть или обсудить с вами ваши действий. Перед тем, как что-то сделать, сначала скажите об этом.

Не Нарушайте Закон

Соблюдайте законы, регулирующие вашу деятельность. Если моральный выбор вынуждает вас нарушить закон, убедитесь, что вы попробовали все возможные варианты, и что общество, скорее всего, будет рассматривать ваши действия, как правильные. Многие случаи нарушения закона являются таковыми, потому что общество решило, что все должно работать определенным способом, даже, если вы уверены, что у вас есть веское оправдание нарушения закона. Само собой, приготовьтесь к тому, чтобы жить с последствиями, которые наступят, когда вас поймают.

Получите Разрешение

Перед тем, как взломать объект, необходимо получить документальное разрешение от владельца объекта или его законного представителя. Это нужно делать во всех без исключения случаях.

Обеспечьте Конфиденциальность Важной Информации

Общество не работает без доверия. Чтобы заслужить доверие, нужно не только действовать честно, открыто и этично, но также не раскрывать важную информацию без предварительного разрешения владельца, особенно, если эту информацию вам сообщили конфиденциально. В целом, чем меньше вы будете разглашать конфиденциальную информацию, тем больше доверия заработаете. Я всегда заключаю с новыми клиентами соглашение о неразглашении (non-disclosure agreement, NDA). Так лучше нам всем. Если вы собираетесь

разгласить чью-то конфиденциальную информацию, убедитесь, что это этично, законно и принесет пользу обществу.

Не Причиняйте Большего Вреда

Клятва Гиппократа должна быть вашим ориентиром не только для поведения в обществе, но и при работе с компаниями или клиентами. Все хакеры должны ее придерживаться. Хакеры и профессиональные пентестеры перед началом работы должны убедиться, что не причинят вреда. Минимизируйте потенциальные сбои в работе. Любую операцию, которая вызовет сбои в работе всегда нужно начинать очень медленно, предварительно проведя множество тестов. А затем используйте такие настройки вашего ПО, которые вызовут минимальный сбой, если есть такая возможность. Если вы совершаете взлом, всегда предупреждайте клиентов (письменно), что ваши действия могут нанести непреднамеренный вред инфраструктуре клиента. Кроме того, не раскрывайте информацию об уязвимостях ПО, предварительно не сообщив о них производителю, и дав ему достаточно времени на выпуск патча. Если сделать наоборот, то это нанесет вред большему количеству клиентов.

Действуйте Профессионально

Стремитесь действовать профессионально во всех сферах. Это не означает, что вам всегда нужно носить костюм. Это означает, что вы должны действовать так, чтобы заслужить доверие, возможно вам даже стоит стать предсказуемым. Доверие также является результатом честной и открытой работы с соблюдением этических норм. Высоких профессионалов отличает умение вести диалог. Вам нужно работать под своим настоящем именем (или из под настоящего профиля, который легко найти в интернете). Плюс, вам не стоит негативно отзываться о других людях и источниках.

Освещайте Путь Остальным

И в конце концов, будьте примером для остальных, и ведите жизнь этичного хакера. Использую свои возможности во благо, и помогайте обществу стать лучше. Покажите остальным, как ваша хакерская этика делает лучше жизнь каждого.

Пусть ваша хакерская деятельность основывается и “хакерской этике” Леви, и на моральных наставлениях, описанных в этой главе. Испытывайте гордость за то, что вы этичный хакер. Все специалисты, представленные в этой книге, являются этичными хакерами, которые не нарушают закон. Они все хорошо зарабатывают. Вы можете стать таким же. Самые умные люди - это не

вредоносные хакеры. Самые умные люди - это защитники, которые их взламывают.