Этичный хакинг, или Ненапрасная жертва кота Твикса

Для чего нужны компаниям белые хакеры и как правильно использовать клиентский опыт в защите от уязвимостей



Текст
ЯНА ШИШКИНА,
ГЛАВНЫЙ РЕДАКТОР **«Б.О»**

Белый хакер, или, на сетевом сленге, белая шляпа (от англ. White Hat), — это специалист по IT-безопасности, который ищет уязвимости IT-систем. В отличие от черных хакеров белые хакеры делают это добровольно, без корыстного интереса или за плату в целях помочь разработчикам сделать их продукты более защищенными.

Об инструментарии ИБ-специалистов, который непрерывно совершенствуется, о законодателях и внесении изменений в регулирование действий белых хакеров в своей статье (ГИПЕР) «Вот тебе, Bug Bounty, и Юрьев день!» рассказал обозреватель «Б.О» **Вадим Ференец.** По его мнению, концепция белого хакерства находится в тренде современного инфополя, которое чутко реагирует на некие из ряда вон выходящие события и происшествия. Они потом становятся мемами, а их герои начинают олицетворять собою либо жертв, либо спасителей мира, привлекая тем самым внимание общественности к разного рода общественным проблемам, но настоящих героев мало кто видел в реальности. Иногда — это не какая-то история серьезного взлома IT-системы, а просто наглядная демонстрация логического сбоя алгоритмов работы IT-платформ или регламентов работы сотрудников компаний с клиентами.

Например, это история несчастного кота Твикса, высаженного проводницей из поезда в мороз, после чего РЖД внесла изменения в правила работы своих проводников, или лайфхак сомнительного обогащения жительницы Красноярска, которая обнаружила баг на Wildberries, позволивший ей получать товары бесплатно. ИБ-эксперт **Алексей Лукацкий** писал об этом кейсе в Telegram: «Если бы эта девушка легально зарегистрировалась в программе Bug Bounty компании Wildberries, то она вполне могла бы получить 500 тыс. рублей за найденные уязвимости и накупить себе всякого разного. Да, это меньше 1,2 млн (полученных ей за продажу ворованных у маркетплейса товаров. — *Ред.*), но зато честно и без риска присесть на 10 лет...». И эти примеры — не про взлом сложнейших IT-систем, а про то, что сейчас компании должны смотреть на свои пользовательские алгоритмы более широко. Почему бы компании Wildberries не промоутировать свою программу Bug Bounty в целях в том числе профилактики подобных преступлений? «Плохо не клади, вора в грех не вводи» — эта старая русская пословица сейчас нуждается в развитии. Как вариант: «Надежно клади — всех на миру́ пробовать взять позови, дабы воры после украсть не могли».

Недавно в интернете мне попалось обращение одной школ по обучению IT-специалистов: «Предлагаем вам сделать выбор между красной и синей таблетками. Мы расскажем, как получить профессию специалиста по кибербезопасности: научиться взламывать информационные системы на законных основаниях и отражать реальные киберугрозы. Чтобы стать специалистом по кибербезопасности, нужно многое уметь. Нео загружал новые навыки напрямую в мозг —и вы тоже можете освоить профессию». Так что, как говорилось в том фильме: “Добро пожаловать в реальный мир”». **Б.О**

