

9. Без письменного разрешения не тестируйте чужие системы: ни «добрые намерения», ни «сообщение постфактум» не освобождают от уголовной ответственности (Китай)

Выгодность исходной версии: высокая

Доказательность А · исходная версия

для свободы

бесплатно

мимоходом

немного силы воли

Частично Китай

Аналог в России не найден

Искали в официальных российских источниках (проверено 08.10.2026), прямого аналога не нашли. Это не значит, что его нет. Китайские условия на Россию не переносите.

Оценки выше относятся к исходной версии; отдельная оценка российского варианта не проводилась.

Простыми словами

Китай — исходная версия. В Китае будет ли обвинительный приговор, зависит от того, было ли разрешение и сколько вы получили, а не от ваших намерений. Получить 500 наборов обычных логинов и паролей, заработать 5000 юаней или причинить другой стороне ущерб в 10 тыс. юаней — уже достаточно для наказания до 3 лет. Если ради доказательства уязвимости заодно выгрузить одну таблицу пользователей, часто уже за один раз получается больше 500 наборов. Даже если логины и пароли у вас уже есть, их использование за пределами разрешённого тоже считается проникновением в систему.

Затраты

Китай — исходная версия. Денег не требует. Прежде чем участвовать в программе SRC компании или в краудсорсинговом тестировании, получите документ, где указаны границы разрешённого, список целей и время, когда можно проводить тестирование. SRC — это собственный центр реагирования компании на угрозы безопасности, который принимает сообщения об уязвимостях от сторонних людей. Как только убедились, что уязвимость действительно есть, остановитесь. Самое трудное — отказаться от «заодно попробую ещё вот это»

Выгода

Китай — исходная версия. Системы обычных компаний и частных лиц относятся к компьютерным информационным системам вне сфер государственных дел, оборонного строительства и передовой науки и техники. За проникновение в такие системы или получение иными техническими средствами данных, которые в них хранятся, обрабатываются или передаются, при серьёзных обстоятельствах назначают до 3 лет лишения свободы либо краткосрочное заключение, со штрафом или только штраф. При особо серьёзных обстоятельствах — от 3 до 7 лет и штраф. У «серьёзных обстоятельств» есть несколько критериев: получение 10 и более наборов данных для подтверждения личности (например, логинов и паролей) в сетевых финансовых сервисах для платежей и расчётов, торговли ценными бумагами, фьючерсами и так далее; получение 500 и более наборов других данных для подтверждения личности; незаконное установление контроля над 20 и более компьютерными информационными системами; незаконный доход от 5000 юаней или экономический ущерб от 10 тыс. юаней. Если указанные выше пороги превышены в 5 раз или более, это уже «особо серьёзные обстоятельства». Официальный пример: в руководящем примере прокуратуры № 36 (检例第 36 号) закреплена формулировка: «Вход в компьютерную информационную систему с использованием логина и пароля за пределами предоставленных полномочий относится к действиям по проникновению в компьютерную информационную систему». Это значит, что, даже если логин и пароль уже были у вас, само их использование за пределами разрешённого считается проникновением. В этом деле трое человек использовали полученные по работе логины, пароли и токены, чтобы из другого места войти во внутреннюю систему компании, скачать данные, не относящиеся к их рабочим задачам, и продать их в интернете. Незаконный доход составил 37000 юаней. Они получили соответственно 4 года, 3 года 9 месяцев и 4 года, каждому также назначили штраф в 40 тыс. юаней (нормы действуют по всему Китаю)

Примечания

Китай — исходная версия. Руководящий пример прокуратуры КНР № 36 (检例第 36 号) сам по себе касается продажи данных ради прибыли. Он приведён только ради формулировки «вход за пределами предоставленных полномочий тоже считается проникновением», а не для утверждения, что за добросовестное тестирование накажут столь же сурово. То, что вы изначально хотели сделать, и то, сообщили ли вы о случившемся постфактум, не отменяет состава преступления. Это может повлиять лишь на суровость наказания и на то, будет ли предъявлено обвинение. Компания может сначала поблагодарить, а потом

обратиться в полицию. Противоречия здесь нет: благодарность не равна разрешению. В 2016 году в Китае один этичный хакер сообщил об уязвимости сайта знакомств «Прекрасная встреча века» (世纪佳缘) на сторонней платформе для сообщений об уязвимостях. Позже компания «Прекрасная встреча века» (世纪佳缘) обратилась в полицию, и его задержали. Компания «Прекрасная встреча века» (世纪佳缘) сообщила журналистам, что обратилась в полицию, потому что кто-то забрал данные. Тогда она не знала, что данные забрал тот же человек, который сообщил об уязвимости. По этому делу есть только сообщения СМИ, нет ни приговора, ни официального сообщения. Официальных сведений о том, чем всё закончилось, нет. На официальных сайтах Верховного народного суда КНР (最高法) и Верховной народной прокуратуры КНР (最高检) также не удалось найти примеры дел о добросовестном тестировании, текст которых можно было бы сверить слово в слово. Поэтому уровень доказательств в этом пункте определён только по статьям закона и критериям наказания. Если собираетесь тестировать, делайте это через открытую программу SRC компании или в рамках оценки безопасности по письменному поручению. Границы разрешённого, цели и временной интервал должны быть записаны в документе. Для доказательства существования уязвимости используйте минимум доказательств, не выгружайте данные массово. В Китае даже если действия не достигают порога уголовного преступления, за них всё равно предусмотрено административное наказание за нарушение общественного порядка, а также запрет на профессиональную деятельность. Размеры штрафов и сроки те же, что в пункте 8 (не запускайте свои программы на чужих компьютерах). О том, что делать после обнаружения уязвимости, см. пункт 10 (сообщайте об уязвимостях по установленным правилам).

Источники

Китай — исходная версия — источники

1. 全国人大 (2020). 刑法 (根据刑法修正案 (十一) 修正, 第二百八十五条第一款、第二款) . jtgl.beijing.gov.cn/jgj/jgxx/flfg/fl/11033925/index.html
2. 最高人民法院、最高人民检察院 (2011). 关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释 (第一条) . ga.sz.gov.cn/ZW GK/ZCFG/ZCJD/content/post_1304363.html (深圳市公安局转载)
3. 最高人民检察院 (2017). 第九批指导性案例 (检例第 36 号, 卫梦龙、龚旭、薛东东非法获取计算机信息系统数据案) . www.spp.gov.cn/spp/jczdal/201710/t20171017_202593.shtml
4. 央广网 (2016-06-29). 白帽子发布漏洞后被抓 世纪佳缘否认“钓鱼”使其上套 (记者赵珂, 实习记者刘香玺) . m.cnr.cn/news/yctt/20160629/t20160629_522531823.html (网页存档 web.archive.org/web/20261005043859/https://m.cnr.cn/news/yctt/20160629_522531823.html)

