СТАРАЯ СКАЗКА НА НОВЫЙ ЛАД

Александр ВЕСЕЛОВ
руководитель отдела технического консалтинга ООО «С-Терра СиЭсПи»

ДА С ПРИСКАЗКАМИ ОТ «С-ТЕРРА»

Жили-были три поросенка. Три брата. Звали их, как вы уже догадались, Ниф-Ниф, Нуф-Нуф и Наф-Наф. Это были продвинутые, современные поросята. Жили они в хороших, крепких домиках, с компьютерами и Интернетом. У каждого была построена целая информационная система, объединяющая их с друзьями.

Весь год занимались они разными важными и необходимыми, как они считали, делами и не задумывались о безопасности своих сетей. Зачем? Ведь вокруг только друзья! Совсем забыли они про злого волка (который мог и данные украсть и их самих съесть) и про строгого медведя (который следил за порядком в лесу и за соблюдением законов).

И вот наступила осень, подул холодный ветер… Да-да, вот такие совпадения. Именно осенью пришли сообщения, что совсем скоро нужно проводить аттестацию систем и для этого приедет с проверкой суровый Топтыгин, а также, что коварный волк поживился информацией в соседнем лесу.

Собрались братья на совет.

— Пора нам подумать об информационной безопасности, — сказал Наф-Наф своим братьям. — Я весь дрожу от страха перед грядущей аттестацией. Давайте построим себе системы защиты и будем спать спокойно.

Но его братья не хотели браться за работу.

— Успеется! Волку наши данные не нужны, а до проверки еще далеко. Мы еще тестированием виртуализации позанимаемся, — сказал Ниф-Ниф и приказал виртуалкам мигрировать в резервный ЦОД.

— Когда нужно будет, я сам построю себе систему защиты, — сказал Нуф-Нуф, открыл ленту новостей в фейсбуке и отлайкал там посты популярного блогера.

— Я тоже, — добавил Ниф-Ниф и вернул виртуалок обратно.

— Ну, как хотите. Тогда я буду один строить себе систему защиты, — сказал Наф-Наф.

Ниф-Ниф и Нуф-Нуф не торопились. Они только и делали, что читали новости и занимались «текучкой».

— Сегодня мы доделаем все «срочные» задачки, — говорили они, — а завтра с утра возьмемся за дело. Но и на следующий день они говорили то же самое. И только когда до приезда медведя остался месяц, ленивые братья взялись, наконец, за работу.

Ниф-Ниф решил, что проще и быстрее всего купить какое-нибудь одно средство защиты. Ни с кем не посоветовавшись, он так и сделал — приобрел антивирус. Очень довольный своей «системой», он направился к Нуф-Нуфу.

Нуф-Нуф тоже очень своеобразно озаботился безопасностью своей инфраструктуры. Он старался скорее покончить с этим скучным и неинтересным делом. Сначала, также как и брат, он хотел просто купить себе антивирус. Но потом вспомнил, что необходим комплексный подход, и добавил в корзину интернет-магазина межсетевой экран с VPN-шлюзом. Пока Нуф-Нуф восхищался своей абсолютной защищенностью, к нему пришел Ниф-Ниф, и они пошли посмотреть — как обстоят дела у Наф-Нафа.

Наф-Наф уже давно был занят постройкой системы безопасности. Он провел обследование, составил модель угроз и техническое задание и теперь не спеша строил себе надежную, современную систему защиты, которая может оградить и от атак злоумышленника, и от штрафов проверяющего. Он обеспечил двухфакторную аутентификацию пользователей, разделил информационную систему на сегменты, реализовал удаленный доступ через внешние сети, не забыв и про регистрацию событий безопасности и реагирование на них. Теперь волк не сможет нарушить конфиденциальность и целостность передаваемой информации. Ниф-Ниф и Нуф-Нуф застали брата за работой.

— Что ты делаешь? — в один голос закричали удивленные Ниф-Ниф и Нуф-Нуф.

А Наф-Наф, как ни в чем не бывало, продолжал настраивать централизованный мониторинг через SIEM систему. Они хотели подразнить Наф-Нафа, но тот даже не обернулся.

— Пойдем, Нуф-Нуф, — сказал тогда Ниф-Ниф. — Нам тут нечего делать!

И два храбрых, но беспечных братца пошли на очередную конференцию.

На ней они так громко рассказывали, как сэкономили на системе защиты время, и деньги, что привлекли внимание волка, который оказался среди слушателей и был не прочь поживиться их информацией.

Ниф-Ниф стал первой жертвой. Пока поросенок работал через удаленный доступ, волк перехватил незащищенный трафик, и данные потекли в его лапы. Ниф-Ниф заметил это и помчался за советом к Нуф-Нуфу.

Едва успели братья обсудить необходимость защиты сетевого трафика, как волк добрался и до Нуф-Нуфа. Но его трафик был защищен VPN-шлюзом, совмещенным с межсетевым экраном, и волк не смог нарушить конфиденциальность информации. А вот для обеспечения целостности использовался алгоритм sha-1 (как недавно выяснилось — не самый надежный). Тут волк пошел на хитрость — изменил передаваемый поросенком трафик, и атака успешно прошла!

Ниф-Ниф и Нуф-Нуф побежали к Наф-Нафу. Они были так напуганы, что ничего не могли сказать. Наф-Наф сразу догадался, что на системы братьев напали. Но ему нечего было бояться со своей суперзащитой. После проверки работоспособности всех компонентов своей системы, он был уверен, что всё в безопасности.

Волк перехватывал и пытался расшифровать трафик, искал уязвимости алгоритма — все напрасно, система выдержала.

Голодному до чужой информации волку ничего не оставалось делать, как убираться восвояси.

И он решил попробовать обойти систему защиты физически — решил украсть устройство, на котором удаленно работал Наф-Наф. Как волк это сделал — до сих пор остается для всех загадкой, но у него в лапах оказался вожделенный тонкий клиент. Но, к огромному его разочарованию, данных на нем не было, так как Наф-Наф использовал специальный загрузочный носитель с встроенным VPN-клиентом, который всегда носил с собой.

* * *

Собрав информацию обо всех трех атаках, братья передали её сотрудникам полиции. Волка нашли и арестовали, а поросята глядели ему вслед и радовались, что они так ловко проучили злого разбойника.

Система Наф-Нафа не только стойко выдержала атаку волка, но и успешно прошла аттестацию. А Ниф-Ниф и Нуф-Нуф сделали себе полноценные системы защиты по примеру брата.

ПРИСКАЗКА 1

В системе Наф-Нафа для защиты удаленного доступа использовались продукты СТерра:

- Многократно проверенный стандартный протокол IPsec — волк не нашел уязвимостей,
- Криптоалгоритмы ГОСТ — волк не нарушил ни конфиденциальность, ни целостность,
- Сертификаты регуляторов — пригодится при аттестации.

ПРИСКАЗКА 2

У Наф-Нафа был не просто VPN-клиент, а специальный загрузочный носитель — СТерра Пост, работающий по технологии среды построения доверенного сеанса.

- Дополнительная аутентификация — носитель используется как токен,
- Изолированная среда — система рабочего места изолирована от системы для удаленного подключения,
- Нет данных на устройстве пользователя — все хранится на сервере.