Безопасность рабочих мест на Linux в 2024 году

Новоселов Михаил Евгеньевич, АО «НТЦ ИТ РОСА», г. Москва, ул. Марксистская, д. 3, стр. 7, m.novosyolov@rosalinux.ru

Информационную безопасность можно разделить на настоящую и «бумажную». К сожалению, эти две области не всегда согласуются между собой. В докладе будут рассмотрены различные аспекты настоящей безопасности использования основанных на Linux операционных систем на различных автоматизированных рабочих местах, как при работе в офисе, так и удаленно:

- настольных компьютерах,
- ноутбуках,
- планшетах,
- мобильных телефонах,
- виртуальных машинах (VDI).

В наши дни основанные на Linux ОС только лишь набирают популярность в качестве ОС для рабочих мест в корпоративном секторе, поэтому существует весьма немного нацеленных на них вредоносных программ (вирусов), а у системных администраторов и специалистов по информационной безопасности мало опыта по борьбе с ними. Большинство из них ни разу не сталкивались с вирусами для Linux.

Прежде чем защищать систему, нужно понять, какова модель угроз, что будем защищать, от чего будем защищаться, чем готовы пожертвовать ради защиты, где находится точка баланса между защитой и удобством использования системы.

Различные архитектурные особенности GNU/Linux, например, отсутствие прав на запуск файла после его скачивания из интернета, усложняют заражение ОС методами социальной инженерии (т. е. когда пользователя убеждают вручную запустить вредоносную программу), но не делают его невозможным.

Пришедшее из мира Windows применение средств антивирусной защиты часто обязательно по нормативным документам, но угрозы, от которых антивирусы способны защитить на Linux, неочевидны, а эвристические и проактивные средства обнаружения вирусов развиты слабо. Антивирус работает с высоким уровнем полномочий в ОС и сам может содержать уязвимости. Необходимо переосмыслить роль антивируса в актуальном ландшафте информационных систем, операционных систем и угроз.

В докладе будет дан субъективный взгляд со стороны разработчика ОС и сопровождающего пакетов в репозитории на текущую ситуацию, методику составления модели угроз, использование антивирусов, будут рассмотрены имеющиеся в Linux и продуктах Росы в частности технические средства противодействия угрозам, дана оценка их влиянию на удобство использование системы.

Отдельный важный аспект настоящей безопасности — это суверенность технологического цикла разработки ОС и всех его компонентов. На примере Android Open Source Project (AOSP) будут рассмотрены проблемы суверенизации огромного технологического стека, будет сделано его сравнение с технологическим стеком GNU/Linux (Роса Хром, Мобайл) с точки зрения суверенности и способности разработчика ОС контролировать все его компоненты, вносить в них любые необходимые правки и проводить собственную техническую политику, в т.ч. по вопросам безопасности.

Отдельно будут рассмотрены десктопные и серверные ОС Роса Фреш и Хром, ОС для повышенной мобильности рабочих мест Роса Барий, построенная на базе того же репозитория ОС Роса Мобайл.