КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2 июня 2022
Иркутск

Импортозамещение и обновление ПО.

#CODEIB

Никифоров Алексей Владимирович

Клуб ИТ-директоров г. Иркутска

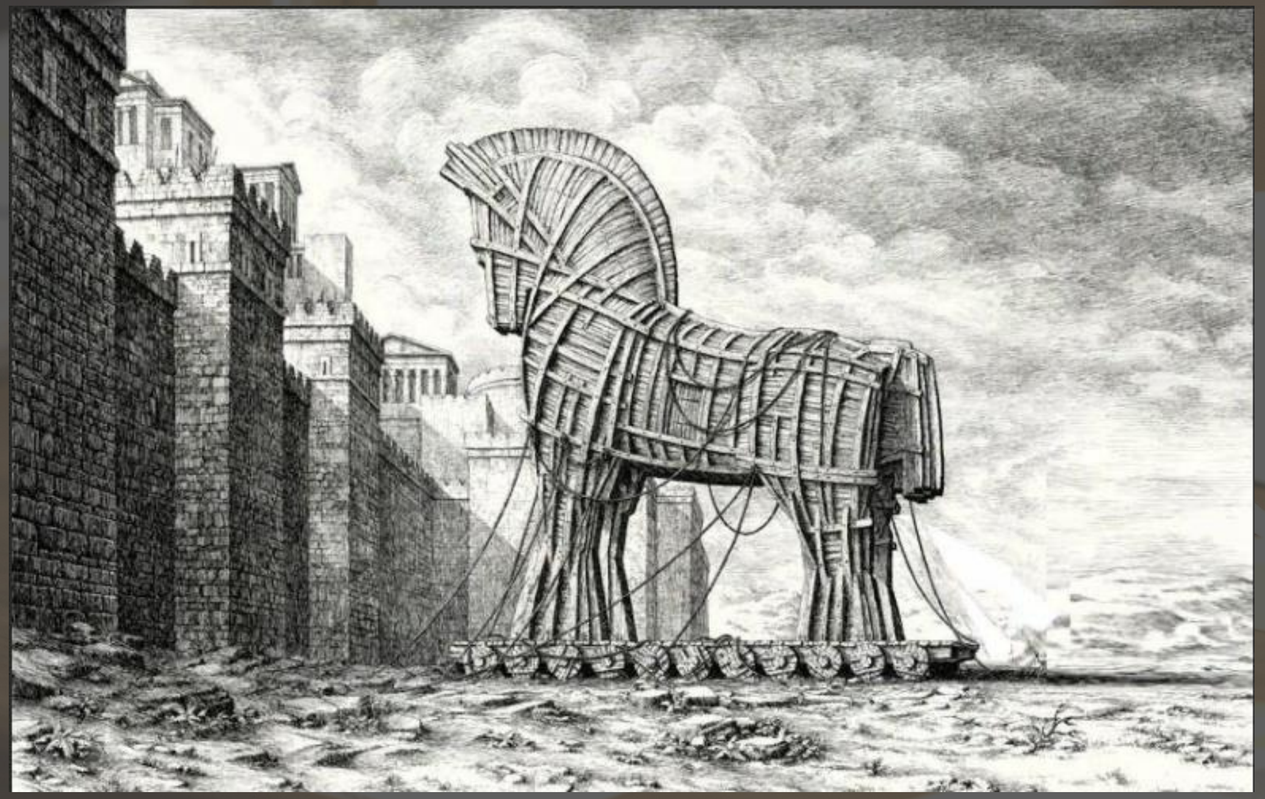
ТЕЛЕФОН: +7 (3952) 91-000-8

EMAIL: anik77896356@gmail.com

Любое ПО содержит уязвимости

Чем дольше не обновляется ПО, тем больше для него шансов столкнуться с вредоносном, эксплуатирующим его уязвимости.

С марта обновления иностранного ПО стали небезопасными.



Пример - закладки в open source библиотеках, реализующие вредоносный функционал по критерию русского ip или часового пояса.

Первая реакция – приостановить обновление иностранного ПО

Но уязвимости накапливаются, надо с этим что-то делать.

- **Мониторим информацию о уязвимостях на профильных ресурсах.**

- **Определяем критичность уязвимости.**
  Место расположения уязвимого ПО в информационной системе, легкость эксплуатации уязвимости.

- **Игнорируем - вводим компенсирующие меры - ставим обновления.**

- **Качаем обновления, проверяя их подлинность по контрольным суммам и цепочкам сертификатов.**

Устанавливаем обновление в тестовой среде

- **делаем резервную копию тестовой среды**
- **настраиваем расширенное журналирование**
- **настраиваем системы мониторинга ИБ в тестовой среде на повышенную чувствительность**
- **проверяем обновление на вирусы**
- **обновляем, проверяем работоспособность обновленного ПО**
- **анализируем сетевой трафик внутри среды и в интернет, целостность тестовой среды по контрольным суммам, появление нового ПО в тестовой среде**

Резервное копирование основной системы

- **Проверяем доступность актуальной резервной копии (дистрибутивы, образы и данные).**

- **Не храним резервные копии там же, где и защищаемые данные.**

- **Не используем для доступа к резервным копиям те же учетные записи, что и для доступа к защищаемым данным**

- **3 копии данных на 2 разных носителях, 1 из них за пределами площадки**

- **Устанавливаем обновление на основную систему.**
- **Мониторим:**
  - **сетевую активность и процессы по эталонным профилям,**
  - **события ИБ.**

Переходим на Российские ОС и ПО

Базальт СПО:
Альт рабочая станция, сервер, сервер виртуализации, образование, СП

ООО Ред Софт:
Ред ОС рабочая станция, сервер, сертифицированная редакция, Ред виртуализация

ГК Astra Linux:
Astra Linux Common Edition, Special Edition, ПК СВ Брест

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2 июня 2022
Иркутск

Импортозамещение и обновление ПО.

#CODEIB

Никифоров Алексей Владимирович

Клуб ИТ-директоров г. Иркутска

ТЕЛЕФОН: +7 (3952) 91-000-8

EMAIL: anik77896356@gmail.com