Astra Linux SE (ОС СН) Смоленск 1.5 Red-Book

Настройка безопасной конфигурации ПК и ОС Astra Linux

1. Настройте BIOS (с целью предотвратить загрузку с внешнего носителя)

1.1. Установите единственным устройством для загрузки ОС - жесткий диск куда была произведена установка ОС.

1.2. Установите "взломостойкий" пароль на BIOS ПК.

1.3 Отключить в BIOS-е Intel SGX (в связи с обнаруженной уязвимостью в механизме).

1.4. Необходимо обеспечить защиту от "незаметного" вскрытия корпуса и встраивания "имплантов" в соединительные кабели периферийных устройств". Для обеспечения защиты могут использоваться специальные корпуса, защитные крышки, пломбы, пломбировочные ленты, для усложнения скрытной установки "имплантов" рекомендуется использование ПК в форм-факторе ноутбук или моноблок.

1.5. При возможности - установите и настройте АПМДЗ на ПК.

1.6. Обеспечьте невозможность физического доступа к жесткому диску на котором установлена ОС, или используйте доступные средства защитного преобразования всего содержимого диска.

1.7. При наличии опций для процессоров Intel Execute Disable Bit (XD-Bit) и для процессоров AMD No Execute Bit (NX-Bit) включите их.

1.8. При наличии на серверах "не доверенных" систем контроля и управления типа ILO,RSA,iDRAC,ThinkServer EasyManage,AMT,iMana - их необходимо отключить, и использовать при необходимости альтернативные решения типа IP KVM.

1.9. Включить secureboot на платформах где это возможно согласно инструкции.

2. Для Intel платформ

2.1 Необходимо устранить уязвимости Intel-SA-00086 в Intel Management Engine(если он инегрирован в процессор) посредством установки обновления микропрограммы Intel Management Engine (производитель оборудования должен обеспечить данную возможность - это либо обновления BIOS, либо ПО для интеграции обновлений). Для частичных проверок используйте: Intel-SA-00086 Detection Tool.

Более подробно:

https://www.intel.ru/content/www/ru/ru/support/articles/000025619/software.html

3. Установите все доступные обновления безопасности ОС Astra Linux

для Astra Linux SE (ОС СН Смоленск):

http://astralinux.ru/update.html

Обновления безопасности и методические указания Astra Linux Special Edition 1.5

4. Настройте загрузчик на загрузку ядра GENERIC и уберите из меню все другие варианты загрузки, включая режимы восстановления.

4.1 Установите "взломостойкий" пароль на загрузчик Grub (устанавливается по умолчанию при установке ОС).

4.2 При использовании архитектур отличных от `Intel` установите пароль на загрузчик согласно документации.

5. При установке рекомендуется создать отдельные разделы / /boot /home /tmp /var/tmp

Раздел */boot* рекомендуется монтировать с опциями `ro` (перед обновлением ядра смонтировать в `rw`)

Разделы */home /tmp /var/tmp* рекомендуется монтировать с опциями `noexec,nodev,nosuid`

6. Установите "взломостойкий" пароли на всех учетных записях в ОС.

6.1 настройте `pam_tally` на блокировку учетных записей при попытках подбора паролей. (настроено по умолчанию при установке ОС)

7. Настройте дисковые квоты в ОС

Для этого установите пакет `quota` настройте */etc/fstab* и используйте `edquota` для установки квот.

8. Настройте ограничения ОС: ulimits

рекомендуемые настройки */etc/security/limits.conf*:

/etc/security/limits.conf

```
#

* hard core 0

#

* hard fsize 50000000

# -(  )

* hard nproc 1000
```

9. Отключите все неиспользуемые сервисы (в т.ч. сетевые) которые запускаются при старте ОС, используя программы:

`chkconfig` и `fly-admin-runlevel` в 1.5

`systemctl systemdgenie` в 1.6

10. Настройте iptables в минимально необходимой конфигурации необходимой для работы

(по умолчанию все запрещено, кроме необходимых исключений)

в 1.5 `iptables ufw`

в 1.6 `iptables ufw gufw`

11. Настройте параметры ядра в /etc/sysctl.conf:

11.1 Отключите механизм SysRq

в */etc/sysctl.conf* добавьте строку

/etc/sysctl.conf

```
kernel.sysrq = 0
```

Перезагрузите ПК, проверьте что установлено значение 0, командой:

```
cat /proc/sys/kernel/sysrq
```

11.2 дополнтельные рекомендуемые параметры

/etc/sysctl.conf

```
fs.suid_dumpable=0

kernel.randomize_va_space=2

net.ipv4.ip_forward=0

net.ipv4.conf.all.send_redirects=0

net.ipv4.conf.default.send_redirects=0
```

12. Заблокируйте исполнение модулей python с расширенным функционалом:

```
find /usr/lib/python* -type f -name "_ctype*" -exec sudo dpkg-statoverride --
update --add root root 640 {} \;
```

13. Заблокируйте макросы в VLC

```
find /usr/lib/ -type f -name "liblua_plugin*" -exec sudo dpkg-statoverride --update --add root root 640 {} \;
```

14. При возможности заблокируйте макросы в Libreoffice

15. Обязательно отключите доступ к консоли пользователям:

(Инструкция для Смоленск 1.5, для 1.6 правила работают из коробки)

Добавьте группу astra-console выполнив команду:

```
addgroup --gid 333 astra-console
```

Создайте файл /etc/rc.local со следующим содержимым:

/etc/rc.local

```
#!/bin/sh -e
chown root:astra-console /dev/{pts,pts/*,ptmx,tty*}
chmod g+rx /dev/{pts,pts/*,ptmx,tty*}
chmod o-rx /dev/{pts,pts/*,ptmx,tty*}
exit 0
```

Добавьте правило в файл /etc/security/access.conf командой:

```
echo "-:ALL EXCEPT astra-console :LOCAL" >> /etc/security/access.conf
```

Включите в /etc/pam.d/login обработку заданных правил командой

```
sed -i 's|.*account.*pam_access.*|account required pam_access.so|' /etc/pam.d/login
```

Для включения доступа к консоли администраторам необходимо добавить их в группу astra-console.

16. Включите контроль цифровой подписи в ELF файлах и в xattr всех файлов,(Режим Замкнутой Программной Среды)

для этого сгенерируйте ключи и подпишите цифровой подписью в xattr все основные файлы и каталоги в корневой ФС.

рекомендуемые каталоги для подписи: */etc /lib /lib64 /lib32 /bin /sbin /boot /root /opt /srv /usr*

16.1 Для включения механизма контроля подписи в ELF:

Установите в файле */etc/digsig/digsig_initramfs.conf*:

/etc/digsig/digsig_initramfs.conf

```
DIGSIG_ENFORCE=1

DIGSIG_LOAD_KEYS=1
```

выполните команду:

```
update-initramfs -u -k all
```

перезагрузите ПК.

16.2 Для включения механизма контроля подписи в `xattr` см. РУК КСЗ п.13.5.2

17. При возможности используйте защитное преобразование данных домашних каталогов с помощью допустимых средств преобразования, или используйте хранение информации на сетевых дисках или сменных носителях.

18. При возможности настройте двухуровневый киоск для пользователя.

см. РУК КСЗ п.15

Как минимум, нужно настроить высокоуровневый киоск для пользователя с помощью утилиты fly-kiosk:

см. РУК КСЗ п.15.6

19. При возможности запретите пользователю подключение сменных носителей.

20. Установите запрет установки исполняемого бита:

```
echo 1 > /parsecfs/nochmodx
echo 1 > /etc/parsec/nochmodx
```

см. РУК КСЗ п.16

21. Настройте систему аудита на сохранение логов на удаленной машине.

Если возможно используйте систему централизованного протоколирования ossec.

см. РУК АДМИН п.15

22. Установите МКЦ > 0 на всех основных файлах и каталогах в корневой ФС. (set-fs-ilev)

(в 1.6 и в 1.5 на апдейтах позже 27-10-2017)

Установку МКЦ рекомендуется проводить после всех настроек безопасности, дальнейшее

администрирование возможно только войдя под высоким уровнем целостности или после снятия МКЦ с ФС командой unset-fs-ilev

Установка МКЦ на 1.5 апдейт 27-10-2017:

см. Мандатный контроль целостности в ОС СН Смоленск 1.5

P.S.

"Взломостойкий" пароль - это пароль не менее 8 символов, не содержащий в себе никаких осмысленных слов(ни в каких раскладках) и содержащий в себе буквы в различных регистрах, цифры и спецсимволы.

23. Включите запрос пароля при каждом выполнении команды sudo, для чего внесите следующие изменения в файл /etc/sudoers:

1. Для того, чтобы для выполнения первой команды sudo требовалось ввести пароль:
   удалить "NOPASSWD:" из строки:

   %astra-admin ALL=(ALL:ALL) ~~NOPASSWD:~~ ALL

2. Для того, чтобы пароль не запоминался для выполнения последующих команд и запрашивался для каждой команды:
   добавить строку

   Defaults timestamp_timeout=0