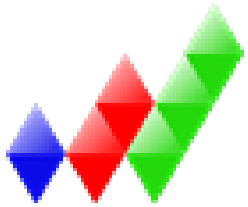
Life2Win

SELinux.
Безопасность в ОС Linux.

Руслан Сафин

24 ноября

PROFIT Securuty Day

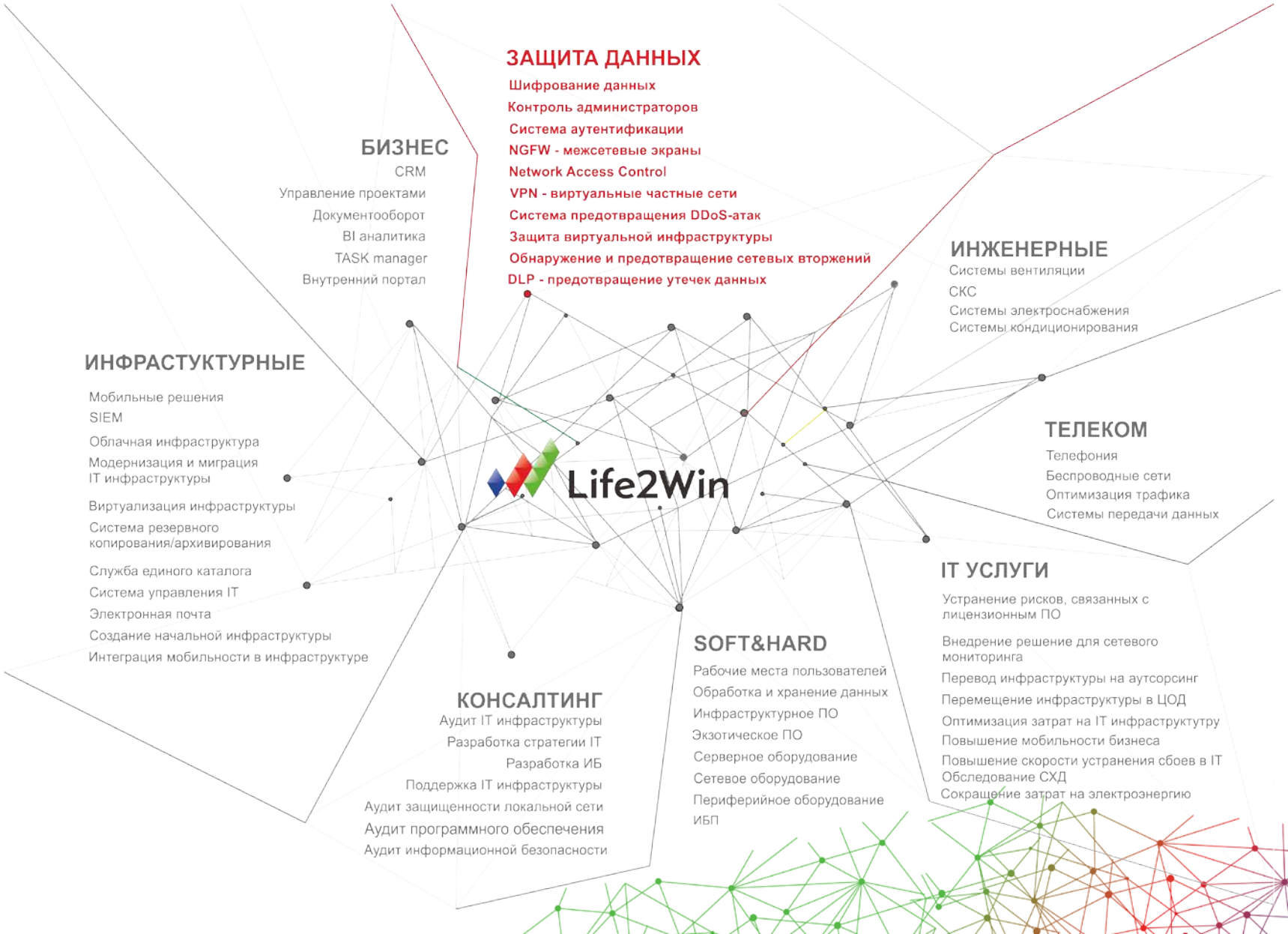


Life2Win

Системный интегратор
инновационных решений
в сфере IT

Life2Win

Наши решения



В основе информационной безопасности лежит управление рисками.

Какие меры принимаются, чтобы реализовать эту концепцию?

- Прозрачность системы
- Принцип наименьших привилегий
- Унификация управления

Содержание

- Что такое SELinux?
  - Стандартная модель безопасности в UNIX-подобных системах
  - Расширения стандартной модели безопасности.
- Как это работает?
  - SELinux: мотивация
  - SELinux: теория
  - SELinux: практика

Security-Enhanced Linux — система принудительного контроля доступа, реализованная на уровне ядра.

Права доступа определяются самой системой при помощи специально определенных политик.

Иными словами, через SELinux нельзя разрешить то, что запрещено через права доступа пользователей или групп. Политики описываются при помощи специального гибкого языка описания правил доступа.

Основа стандартной модели безопасности - система привилегий.

В системе существует набор пользователей.

```
# cat / etc / passwd | sed ' s /:.*// g '
root
bin
daemon
adm
...
```

Множество пользователей разбивается на подмножества,

называемые группами.

Стандартная модель безопасности

В системе существует множество файлов. У каждого файла есть владелец (один из пользователей) или группа владельцев.

С каждым из файлов ассоциирован набор прав доступа.

Набор прав включает в себя:

- Права владельца
- Права группы владельцев
- Права остальных пользователей

```
- rw - r -- r -- 1 root root / etc / passwd
```

Стандартная модель безопасности

Любой процесс, запущенный пользователем, обладает всеми правами этого пользователя.

Это потенциальная точка уязвимости.

Администратор не может в полной мере контролировать действия пользователя. Например, пользователь вполне способен дать всем остальным пользователям права на чтение собственных конфиденциальных файлов, таких как ключи SSH.

Что может пойти не так?

Процессы могут изменять настройки безопасности.

Например, файлы, содержащие почту пользователя должны быть доступны для чтения только одному конкретному пользователю, но почтовый клиент вполне может изменить права доступа так, что эти файлы будут доступны для чтения всем.

Процессы наследуют права пользователя, который их запустил.

Например, зараженная трояном версия браузера Firefox в состоянии читать SSH-ключи пользователя, хотя не имеет для того никаких оснований.

Как следствие:

Любое приложение имеет доступ к любым ресурсам, к которым имеет доступ пользователь.

- Например, skype имеет право на доступ к файлам в /.mozilla/firefox.
- Если баг в веб сервере Apache позволяет повысить привилегии для учетной записи root - вся система находится под угрозой.
- Нет простого метода, который позволил бы устанавливать для каждого пользователя необходимый минимум привилегий.

В результате, компрометация любого из пользовательских приложений позволяет злоумышленнику получить все привилегии пользователя.

```
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "Htf4CRBDpVhcwwC9\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 2 opened (10.0.0.100:4444 -> 10.0.0.3:38149) at Mon May

whoami
distccd
```

Почему SELinux?

- SELinux следует модели минимально необходимых привилегий для каждого сервиса, пользователя и программы.
- «Запретительный режим» установлен по умолчанию.
- Пользователь, программа или сервис получить доступ к неразрешенному контенту - отказ в доступе, попытка зарегистрирована в журнале.

SELinux увеличивает степень безопасности всей системы.

- Создание и настройка списка программ, которые могут читать ssh-ключи.
- Предотвращение несанкционированного доступа к данным через mail-клиент.
- Настройка браузера таким образом, чтобы он мог читать в домашней папки пользователя только необходимые для функционирования файлы и папки.

Type Enforcement (TE): основной механизм контроля доступа, используемый в целевых политиках. Позволяет детально, на самом низком уровне управлять разрешениями. Самый гибкий, но и самый трудоемкий для системного администратора механизм.

Role-Based Access Control (RBAC): права доступа реализуются в качестве ролей. Роль - разрешения на выполнение определенных действий одним или несколькими элементами системы над другими частями системы. Является дальнейшим развитием TE.

Multi-Level Security (MLS): многоуровневая модель безопасности. Всем объектам системы присваивается определенный уровень доступа. Разрешение или запрет доступа определяется соотношением этих уровней.

Life2Win

Существует готовая политика SELinux, которая содержит описание типов и профилей для большого числа приложений.

Исходные коды политики можно найти в $SELINUX_POLICY_SRC/policy/modules/

Дерево исходных кодов политики содержит:

- admin – Профили административных утилит (su, netutils, rpm, apt, etc.)
- apps – Профили приложений (mozilla, wireshark, java, etc.)
- kernel – Профили стафа, относящегося к ядру
- roles – Описания ролей для ролевого контроля доступа
- services – Различные сервисы (ssh, snmp, jabber, etc.)
- system – Системные приложения (init, logging, udev, xen, etc.)

Life2Win

SELinux

- Беспрецедентный контроль инфраструктуры
- Мощный инструмент логирования
- Защита он несанкционированного действия
- Гибкость и простота в управлении
- Работает «из коробки»

Спасибо