Уязвимости технологических систем операторов связи

Вспомогательные системы

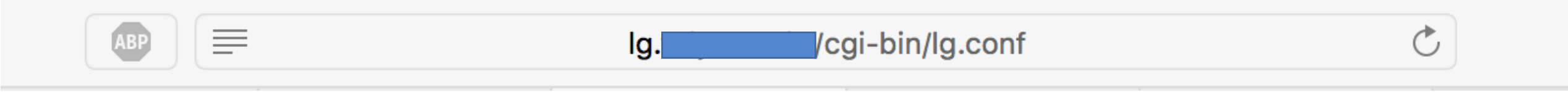
- Configuration Management
- Incident Management
- Мониторинг
- Looking Glass
- …

Сеть – критический элемент инфраструктуры оператора

- Несанкционированный доступ к конфигурациям оборудования
  - Настройки безопасности
  - Информация о клиентах
  - Доступ к персональным данным
  - Доступ к внутренней сети предприятия
  - Лицензионные данные оборудования
- Уничтожение конфигурации
  - Длительная недоступность услуги для абонентов
  - Доступ к резервным копиям конфигураций

Типовая ошибка: Looking Glass

- Доступно из публичного интернета
- Содержит пароли на оборудовании
- Готовые решения уязвимы по умолчанию



```
<Router_List>

        <Separator>Selecione</Separator>

        <Router Name="Tely - Joao Pessoa - PB" Default = "yes" OSType = "JunOS">
                <URL>telnet://lg:s3j[redacted]2@187.33.245.153</URL>
        </Router>

        <Router Name="Tely - Campina Grande - PB" OSType = "JunOS">
                <URL>telnet://lg:s3j[redacted]2@177.75.76.137</URL>
        </Router>

        <Router Name="Tely - Patos - PB" OSType = "JunOS">
                <URL>telnet://lg:s3j[redacted]2@177.75.74.65</URL>
        </Router>

        <Router Name="HostDime - Joao Pessoa - PB" OSType = "Zebra">
                <URL>telnet://lA[redacted]r@187.33.254.102:2601,2605</URL>
        </Router>

</Router_List>
```

Внутренняя сеть

Как избежать?

- ACL на управляющие интерфейсы
  + Самое очевидное
  + Все делают так ☺
  - Легко забыть на одном из маршрутизаторов
- Использование механизмов ограничения доступа TACACS
  - Сложнее конфигурация
  + Централизованное изменение
  + Невозможно «потерять» маршрутизатор

Контроль служебных учетных

- Сколько на сети служебных учетных записей?
- Сколько используется SNMP-community?
- А сколько из них read-write?