Уважаемые клиенты, ГК «Агат-РТ» информирует Вас о безопасности настроек оборудования!

Технология хакерских атак, как правило, типичная – сканирование порта 5060, попытка зарегистрироваться на сервере как внутренний пользователь и совершение исходящих вызовов. Для своих атак хакеры выбирают выходной или праздничный, а время – с часу ночи до пяти утра. Попытка регистрации, как правило, простая и без подбора пароля. В качестве параметров авторизации хакеры используют перебор номером 101, 102, 103, 104 и т.д. и 1001, 1002…

Защита VoIP соединений и сервера телефонии или IP-АТС от несанкционированного доступа лежит в зоне ответственности пользователя. Производитель не несет ответственности за несанкционированные соединения через телефонную станцию.

Так как защитить себя от возможных атак и финансовых потерь?

Защита на самом деле простая. Общий смысл защиты заключается в том, чтобы исключить возможность регистрации внутреннего абонента с внешней интернет сети на сервере телефонии. Если существует необходимость, чтобы внутренний абонент телефонии все же мог регистрироваться на сервере IP-телефонии с внешней интернет сети, то реализовывать такую возможность надо с использованием технологии VPN подключения.

Для защиты IP-АТС Агат UX достаточно выполнить элементарные правила обеспечения безопасности АТС:

1. Не используйте логины и пароли по умолчанию для доступа к АТС.
2. Не используйте совпадающие логины и пароли для абонентов SIP-прокси сервера.
3. Для входящих и исходящих вызовов используйте разные таблицы маршрутизации.
4. В таблицах маршрутизации для исходящей связи не указывайте ненужных направлений или общих шаблонов для всех вызовов.
5. Используйте PIN коды доступа к конфигуратору или аппаратную защиту IP-АТС от доступа конфигуратором.
6. Контролируйте количество и направления звонков проходящих через АТС посредством SMDR записей (подробнее см. Руководство пользователя системы учета вызовов).
7. Для абонентов встроенного SIP-прокси сервера в дереве конфигуратора рекомендуем установить следующие варианты аутетификации:
    - в меню **SIP – SIP регистратор** включите **режим проверки пароля – проверять только персональный** (отключение проверки пароля позволит звонить через Вашу АТС всем SIP клиентам).
    - в меню SIP – SIP регистратор **включите режим аутентификации – Проверять среди зарегистрированных.**
    - Если вы в меню **SIP - вкладка Общие - Способ маршрутизации** поставили одну из ТМ, то лучше убрать из этой ТМ выход в город. В случае, если по каким-либо соображениям выход в город для этой ТМ должен присутствовать – настройте для этого соединения проверку АОНа и разрешение звонков только для определенных абонентов, либо настройте выход в город не через стандартный префикс (обычно стандартный префикс – 9ка).
8. По аналогии с предыдущим пунктом можно запретить исходящие звонки в ночное время суток и в выходные, что не позволит пустить трафик через АТС в нерабочие часы, пока Вы не имеете возможности контролировать соединения через АТС.

Дополнительные элементы защиты для всех устройств IP-телефонии

9. Средствами сетевых маршрутизаторов и фаерволов запретите весь VoIP трафик со сторонних IP адресов.
10. Для регистрации SIP абонентов используйте нестандартные порты, которые средствами NAT в ЛВС можно преобразовать в типовые порты для установки SIP соединений.