БЕЗОПАСНОСТЬ В IP-ТЕЛЕФОНИИ

ЕСЛИ ВАША IP-АТС ДОСТУПНА ИЗ ИНТЕРНЕТА, ЭТА ИНФОРМАЦИЯ ДЛЯ ВАС

Последнее время наблюдается рост численности случаев мошенничества при использовании IP телефонии. Соблюдение простейших условий поможет Вашей Организации не понести большие убытки, связанные с действиями хакеров.

Выполнение данных рекомендаций значительно снизит риски, связанные с нарушением конфиденциальности Ваших данных, возможности проникновения в сеть Вашей организации при разворачивании IP-телефонии, минимизирует риски связанные с перепродажей трафика, с возможностями фрода.

Зачастую угрозы проникновения в сеть возможны из-за неправильной настройки оборудования на стороне клиента, из-за несоблюдения элементарных требований безопасности при работе с информационными технологиями.

1. ПЕРВООЧЕРЕДНЫЕ МЕРОПРИЯТИЯ

- ☐ **Смените авторизационные данные используемые по умолчанию на оборудовании (связки логин/пароль).** Большинство атак реализуется именно путем использования данных установленных по умолчанию (логин admin, пароль admin; логин cisco, пароль cisco и т.п.). Используйте сложные пароли, устойчивые к перебору- большие буквы, маленькие буквы, цифры, спецсимволы. Не используйте одинаковые данные для доступа к разным ресурсам: уникальные связки для SIP аккаунта, для доступа к оконечному оборудованию, авторизации Asterisk, доступа в личный кабинет и WEB-интерфейсу
- ☐ При отсутствии необходимости звонков на международные\междугородние номера, **отключите данную услугу** на своей стороне, либо на стороне оператора, связавшись с Вашим персональным менеджером.
- ☐ Установите на всех местах откуда осуществляется работа с оборудованием **современный антивирус** с регулярно обновляемыми базами.
- ☐ Всегда **используйте последние стабильные прошивки** используемого оборудования и программного обеспечения. Уязвимости в ПО- второй по популярности способ получения несанкционированного доступа к системам IP телефонии.

2. ПРИ НЕОБХОДИМОСТИ ИСПОЛЬЗОВАНИЯ ФУНКЦИЙ МЕЖДУНАРОДНОЙ СВЯЗИ

- ☐ Установите максимальную длительность сессии на международные\междугородние номера, к примеру 200-300 секунд, учитывая многоканальность и специфику Вашей Организации.
- ☐ Установите запрет звонков на фродоопастные направления- Чили, Перу, Филиппины и т.п.
- ☐ Настройте звонки по международной связи только с использованием пинкодов.

3. НА ЧТО СТОИТ ОБРАТИТЬ ВНИМАНИЕ

- ☐ Настройте регулярные информационные сообщения о происходящей подозрительной активности- попыток перебора паролей, попыток звонки на международные номера, попыток доступа к оборудованию.
- ☐ Меняйте все связки логин/пароль на оборудовании при смене обслуживающего персонала. Человеческий фактор- третья по распространённости причина информационных угроз.
- ☐ Грамотно настройте Вашу внутреннюю сеть- разрешение на международные звонки только с определенных внутренних номеров, использование межсетевых экранов при доступе к оборудованию из Интернета, администрирование оборудования с конкретных IP устройств и т.п.

Наши специалисты всегда готовы ответить на любые Ваши вопросы и помогут с настройкой оборудования. Номер Техподдержки: 8 800 333 9000