БАНК САНКТ-ПЕТЕРБУРГ

Банк высокой культуры

Какие ИБ-решения должны быть внедрены в компании, чтобы обеспечить безопасность удаленной работы

Скородумов Анатолий Валентинович

Начальник управления по обеспечению информационной безопасности

Использование удаленного доступа

- Различного рода администраторы
- Руководство организации и менеджеры разного уровня
- Мобильные сотрудники

Что существенно изменилось?

- Масштабы. Удаленно работают до 90% сотрудников организации. Работают в постоянном режиме по 8 часов в день
- Уровень доступа, критичность выполняемых операций. 90 процентов операций, включая критичные выполняются удаленно
- Процент сотрудников, работающих с личных устройств

70-80% ПОЛЬЗОВАТЕЛЕЙ РАБОТАЮТ В НЕПРИВЫЧНЫХ УСЛОВИЯХ!!!

Основные угрозы удаленного доступа

- Утечка данных (в результате несанкционированного доступа к пользовательскому устройству или из-за недобросовестного поведения самого сотрудника)
- Проведение атак на корпоративные системы через пользовательские устройства
- Заражение корпоративных систем вредоносным ПО
- Невозможность удаленной работы из-за недоступности сервиса удаленного доступа

Корпоративные и личные устройства

Требования к корпоративным устройствам:

- ОС с наличием актуальных обновлений
- Антивирус с актуальными базами + EDR+DLP
- Шифрование жесткого диска
- Ограничения по доступу в Интернет
- Отсутствие у пользователя административных прав доступа

Требования к личным устройствам – АНАЛОГИЧНЫЕ, НО……

Основные принципы безопасного удаленного доступа

- Двухфакторная аутентификация
- Защищенное соединение
- Проверка подключаемого устройства на соответствие политикам ИБ
- Запрет на файловую передачу данных, использование буфера обмена, присоединения дисков удаленного компьютера и т.п.
- Контроль за подключениями и действиями удаленных пользователей

Необходимые ИБ решения

- Антивирус для установки на личные устройства пользователей
- Сервер удаленного доступа с функцией NAC
- Решение PAM для удаленного доступа критичных работников
- SIEM для корреляции событий и выявления инцидентов
- DLP с хостовым агентом для контроля видеоконференций
- Антивирус + EDR на пользовательских компах внутри организации
- Внешний сканер безопасности
- WAF, если используете WEB-публикацию приложений
- Защита от DDOS узлов удаленного доступа

Безопасность систем видеоконференцсвязи

“Несколько тысяч записей личных видеозвонков пользователей сервиса видеоконференций Zoom утекли в Сеть. Ролики появились в открытом доступе на платформах YouTube и Vimeo, сообщило издание The Washington Post. ….Программа Zoom не ведет запись видеозвонков по умолчанию, однако организаторы конференций могут активировать запись и сохранить ее либо в облачном хранилище сервиса, либо в памяти своего устройства. Данный процесс осуществляется без согласия участников, хотя они и получают уведомление о начале записи.
Главной проблемой Zoom является то, что сервис присваивает видеоконференциям открытые идентификаторы и не шифрует подключение и в ходе online-поиска можно обнаружить большое количество записей. По данным некоторых экспертов, таким образом они нашли более 15 тыс. записей.”

- Слабый контроль за созданием конференций
- Отсутствие ограничение по обмену данными внутри конференций
- Слабый контроль состава участников конференций
- Отсутствие возможности ограничить запись конференции
- Наличие уязвимостей

Что еще может нам помочь?

ТО, ЧТО ЭТО ДОЛГО НЕ ПРОДЛИТЬСЯ!

БАНК
САНКТ-ПЕТЕРБУРГ

Банк высокой культуры

Скородумов Анатолий Валентинович

Телефон (812) 329-50-64

Благодарю за внимание!