ДЗ 6

Наиболее чувствительная информация:

- доступ администратора (учетные данные, шифрование)

- доступ пользователей (учетные данные, шифрование)

- контент (архив)

Наиболее уязвимые сегменты:

Доступ из интернет – клиент и мобильный клиент

Основное:

1. DMZ заказчика не защищена WAF, а клиенты имеет доступ напрямую – поставить на вход/выход DMZ, в том числе для доступа из LAN (inside заказчика). Через сервер WEB есть риск получить атаку на сервер приложений и на сервер баз данных внутри DMZ.
2. Также WAF ставим на все сегменты инфраструктуры (сервер приложений RichCall, сегмент сети RichCall, который находится в интернете, сегмент сети администраторов заказчика.
3. Очевидно, что в каждом сегменте на каждой рабочей станции и на каждом сервере должен стоять антивирус.
4. На сегменте inside заказчика в сети администратора и рабочих станций оператора должна стоять DLP система, если эти рабочие станции имеют выход наружу (в интернет, USB носители итд)
5. Наверное, должна существовать политика обновления статических DHCP адресов на рабочих станциях операторов с соответствующим обновлением доступов в DMZ.
6. Для постоянного анализа возможных угроз в DMZ также ставим SIEM систему с дальнейшим апгрейдом SOAR в случае наличия значимого количества инцидентов
7. Ставим IPS системы на всех сегментах инфраструктуры, чтобы обнаруживать и предотвращать возможные атаки как снаружи, так и изнутри.
8. Можно повысить безопасность пользовательских данных и снизить риск фрода, введя двухфакторную аутентификацию клиентов