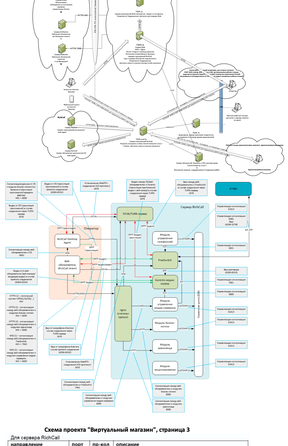
# ДЗ №07 - Денис

Урок 7. IT-инновации в бизнесе. Модели, виды, системы. Уязвимости, подходы к защите и аналитика

**1. Составить свое экспертное мнение по поводу защищенности планируемой реализации, IT-инфраструктуры и ландшафта, составить предложения по модернизации схемы и внедрению средств защиты (процессы защиты) в т.ч. и исходя из материалов 2-6 уроков.**



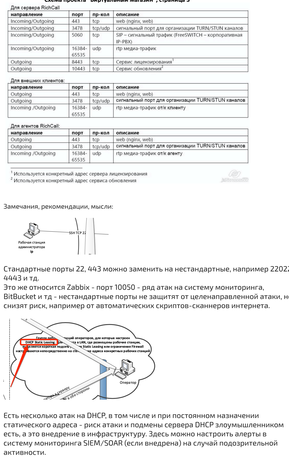


**Схема проекта "Виртуальный магазин", страница 3**

Для сервера RichCall:

| направление | порт | пр-кол | описание |
|---|---|---|---|
| Incoming/Outgoing | 445 | tcp | web (nginx, web) |
| Incoming/Outgoing | 3478 | tcp/udp | сигнальный порт для организации TURN/STUN каналов |
| Incoming/Outgoing | 5060 | tcp | SIP – сигнальный пробив (FreeSWITCH – взаимодействие IP-PBX) |
| Incoming/Outgoing | 16384 - 65535 | udp | rtp медиа-трафик |
| Outgoing | 8443 | tcp | Сервис лицензирования[1] |
| Outgoing | 10443 | tcp | Сервис обновления[2] |

Для внешних клиентов:

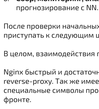
| направление | порт | пр-кол | описание |
|---|---|---|---|
| Outgoing | 445 | tcp | web (nginx, web) |
| Outgoing | 3478 | tcp/udp | сигнальный порт для организации TURN/STUN каналов |
| Incoming /Outgoing | 16384 - 65535 | udp | rtp медиа-трафик отв клиенту |

Для агентов RichCall:

| направление | порт | пр-кол | описание |
|---|---|---|---|
| Outgoing | 443 | tcp | web (nginx, web) |
| Outgoing | 3478 | tcp/udp | сигнальный порт для организации TURN/STUN каналов |
| Incoming /Outgoing | 16384 - 65535 | udp | rtp медиа-трафик отв агенту |

[1] Используется конкретный адрес сервера лицензирования
[2] Используется конкретный адрес сервера обновления

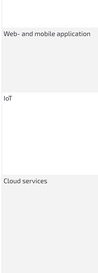
Замечания, рекомендации, мысли:



Стандартные порты 22, 443 можно заменить на нестандартные, например 22022, 4443 и тд.
Это же относится Zabbix - port 10050 - рад атак на систему мониторинга, BitBucket и тд - нестандартные порты не защитят от целенаправленной атаки, но снизят риск, например от автоматических скриптов-сканеров интернета.

Есть несколько атак на DHCP, в том числе и при постоянном назначении статического адреса - риск атаки и подмены сервера DHCP злоумышленником есть, а это внедрение в инфраструктуру. Здесь можно настроить алерты в систему мониторинга SIEM/SOAR (если внедрена) на случай подозрительной активности.

ПО ФЗ замечания:



На этих серверах могут обрабатываться *личные данные*. Так же необходимо знать какой именно видеоконтент сохраняется.

Пробежимся по CIS BACIS:

1. ***Инвентаризация и контроль технических средств***. *Здесь учет девайсов на местах - рабочих станций операторов, серверов, девайсов - камер, микрофонов.*
2. ***Инвентаризация и контроль ПО***. Инфраструктура не самая сложная и запутанная, но объемы трафика (видео/аудио) это достаточно уязвимое место - риск утечек, те человек самое слабое место всегда. Здесь стоит задуматься о SIEM системе, которая позволит сфокусироваться на контроле актуальных версий ПО на всех серверах во всех зонах, особенно в зоне internet. Так же это первый шаг к анализу трафика на предмет утечек - начинаем собирать биг дату.
3. **Непрерывное управление уязвимостями**. Здесь будет очень замечательно апнуть SIEM до SOAR и сфокусировать анализ на самых слабых местах - далее по ходу накопления информации, BIG DATA - можно внедрить системы МО/ИИ для оптимизации и прогнозирования угроз, распознавания утечек - здесь надо конечно оценивать бюджет и масштабы, трафик может быть огромный.
4. **Контроль администрирования**. Инфраструктура как отметили - не самая сложная, но в настроенных под инфраструктуру SIEM/SOAR это будет оптимально.
5. **Защищенные настройки мобильных устройств, ноутов, АРМ, планшетов, серверов**. Помимо безопасной конфигурации устройство - мы же можем сфокусировать антивирусный модуль сканирования в SIEM в случае обнаружения угроз применить меры незамедлительно.
6. **Сбор, мониторинг, анализ событий безопасности**. SOAR + анализ-прогнозирование с NN.

После проверки начальных этапов оптимизации защиты по best practice можно приступать к следующим шагам.

В целом, взаимодействия грамотно организованы по https, имеется шлюз, vpn.

Nginx быстрый и достаточно гибкий, имеет опции настройки как прокси, так и reverse-proxy. Так же имеет модуль WAF, позволяющий фильтровать специальные символы программно, поникая риск тех же xss, SQL-инъекций на фронте.

Если это Виртуальный Магазин - предположительно, есть платежи, есть транзакции защиту которых так же необходимо обеспечить согласно стандартам. Если есть опции оплаты через мобильные приложения - обеспечить необходимую защиту, внедрить, например токены. Система анти-фрода - возможно, требуется уточнение. Это может быть атака, например по телефону - распознавание голоса, аналитзатор, так же здесь может эффективно бороться ИИ - опять же, зависит от масштабов - если это Амазон - один подход, если это магазинчик частного плана - совершенно другой бюджет и подход к защите.

Пентестинг инфраструктуры - как плановый, так и совершенно внезапный, в том числе и социальная атака на персонал - на предмет ценной информации или же это несанкционированная транзакция. Многое зависит от того что именно происходят на контуре.

Практическое задание к схеме 6 / 7 уроков:

Сразу сведем в табличку:

| Наименование средства защиты | Цели, прикладное размещение и необходимость использования |
|---|---|
| BigData | Несомненно рекомендуется внедрение в данную инфраструктуру для отказоустойчивости, снижения рисков, обеспечения непрерывности БП. |
| NN, AI, machinelearning | Для прогнозирования всевозможных рисков и потенциальных угроз рекомендуется внедрение - можно сфокусировать обучение на накопленных данных и со временем прогнозы будут точнее и точнее, что позволит подключать дополнительные вектора для анализа и прогнозирования, оптимизировать инфраструктуру, более безопасно масштабировать проект.<br>Как и многое - все зависит от бюджета и целей бизнеса. |
| Web- and mobile application | Клиент и мобильный клиент присутствуют. Риск xss, бруттфорса, инъекций и тд.<br>Тщательная проверка конфигурации сервера, бд, антибруттфорса, внимательное экранирование входных данных, по возможности отключить trace-запросы.<br>В тонких местах настроить алерты SOAR/SIEM с подключением прогнозированся с использованием NN. |
| IoT | В данной инфраструктуре наблюдается взаимодействие с IoT устройствами. Высокий риск угроз ИБ-разного уровня, например, DDoS, бруттфорс. Организовать защиту платформы в соответствии с best practice.<br><br>Но так как рынок IoT только развивается, стандарты и сертификации еще не сформированы - будет крайне полезно сочетать SOAR и МО, сфокусировать на слабые места: вебкамеры, микрофоны - могут быть простые и сложные устройства с элементами IoT. |
| Cloud services | Требуется уточнение. Видимо, не без облачной архитектуры - необходимо знать конкретную модель. Угрозы те же, что были выше + риск атаки на гипервизоры, облачную API, виртуальные машины.<br>Защита фокусируется:<br><br>- Обеспечение нативной безопасности.<br>- Использование разных форм-факторов.<br>- Обеспечение централизованного управление.<br>- Пентестинг.<br>- Создание облачных сервисов с учетом стандартизации и best practice |
| Виртуализация и контейнеризация | Видим докер в бою.<br>Защищаем:<br>Эксплуатация достоверных образов.<br>Использование Docker Content Trust.<br>Использование Docker Bench Security.<br>Создание нативных настроек безопасности хостовых систем.<br>Создание нативных настроек улучшения безопасности Docker.<br>Ограничение использования системных ресурсов.<br>Мониторинг и сканирование CVE-уязвимостей.<br>Подпись и проверка образов.<br>Использование фиксированных тегов и исключение чувствительной информации из контейнеров.<br>Многоэтапная сборка и управление привилегиями. |

*Задание выполнено!*

2020.11.20 19:38