Трубная Металлургическая Компания

Москва 2022 г.

«Проблемные вопросы обеспечения безопасности КИИ в период пандемии Covid-19» (ТБ-ФОРУМ 2022)

1. Краткое описание ситуации.

- **Массовый перевод персонала на режим удаленной работы (по данным Минтруда в 2021г. более 3 млн. россиян) поспособствовал резкому росту применения технологий дистанционной работы: по данным исследования Microsoft рост он- лайн трансляций в MS Teams в 2021 г. составил более 148%, а совокупный прирост использования облачных сервисов на базе MS Azure составил более 775%!**

- **Сложившаяся ситуация качественно повлияла на уровень и значимость технической поддержки и сопровождения как корпоративного сегмента ИТ-инфраструктуры Предприятий, так и промышленного (АСУТП).**

- **Активизация кибер- атак на он-лайн открытые сессии дистанционного персонала, включая их личное оборудование.**

- **Перевод технического персонала подрядных Организаций сегмента АСУТП на дистанционный режим.**

2. Основные проблемы ИБ КИИ на дистанте.
Чего не следует допускать.

1. **Перевод ключевых технических ИТ-специалистов АСУТП на дистанционный режим работы даже в тех случаях, когда инфраструктура позволяет.**
2. **Перевод работников информационной безопасности сегмента АСУТП на удаленный режим.**
3. **Использование личной компьютерной техники работниками АСУТП, выведенных на дистант.**
4. **Открывать УД к объектам ЗОКИИ (как подрядчикам, так и собственному дистанционному персоналу).**

3. Основные риски и вектора атак.

Основные ИБ- риски в период пандемии для сегмента КИИ:

- проникновение ВПО через удаленную открытую сессию;
- перехват управления оборудованием и ПО злоумышленниками через удаленную открытую сессию;
- получение производственных данных (статистика, метрология, технологические параметры процессов) третьими лицами.

Основные и наиболее вероятные вектора атак для КИИ:

- эксплуатация уязвимостей корпоративного сегмента сети Предприятия, как отправной точки целевой атаки на АСУТП (ОКИИ/ЗОКИИ) в случае сетевой связанности двух сегментов;
- эксплуатация уязвимостей ИТ-инфраструктуры подрядных организаций, сопровождающих АСУТП Предприятия в удаленном режиме, как точки проникновения в ЛВС Предприятия.

4. Почему?

Потому что - LOG4SHELL

(CVE-2021-44228) — это уязвимость нулевого дня в библиотеке Log4j, популярной среде ведения журналов Java, включающая выполнение произвольного кода. Имеет наивысший, 10-й уровень опасности по CVSS)

Уязвимые сервисы и ИС корпоративного сегмента, позволят злоумышленникам про- эксплуатировать уязвимость, закрепиться в Организации и проникнуть в промышленный сегмент АСУТП!

5. Что необходимо.

1. Отключить доступ из сети Интернет к серверному оборудованию Предприятия, где в этом нет необходимости.
2. Установить на все промежуточные сервера удаленной авторизации антивирусное ПО.
3. Уделить особое внимание решениям от VMware; Apache; Jawa и произвести необходимые мероприятия по патч- менеджменту.
4. Активно использовать имеющиеся возможности SOC-центра для выявления подозрительной активности внутри ИТ- инфраструктуры Предприятия.
5. Сменить модель технического сопровождения АСУТП (особенно ЗОКИИ) подрядчиками с он- лайн формата, на физическое присутствие внутри Предприятия.

Подготовил: Севостьянов А.В.
Начальник УИБ СЭБ ТМК
Москва, 2022

**Узнай больше
о компании ТМК**

**ТМК eTrade
Интернет-магазин труб**

**Премиальные резьбовые
соединения ТМК UP**