Мониторинг событий информационной безопасности: выявление таргетированных атак

Ким Вячеслав

Заместитель генерального директора

ООО «Информационный центр»

8 (423) 240-48-66 доб.7007

kim.vs@ic-dv.ru

Простыми словами:

Мониторинг – сбор событий, их обработка и анализ.

(это регистрация событий безопасности и их отслеживание, выявление компьютерных инцидентов, информирование о компьютерных инцидентах, анализ компьютерных инцидентов)

КИИ – по закону (с разделением на значимые и незначимые) и на практике.

(здравоохранение, наука, транспорт, связь, энергетика, банковская сфера, топливно-энергетический комплекс, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, а также организации, обеспечивающие взаимодействие систем или сетей КИИ)

Таргетированные атаки – подготовленные и направленные атаки на конкретные объекты с определенными целями.

(непрерывный процесс несанкционированной активности в инфраструктуре атакуемой системы, управляемый киберпреступником в режиме реального времени)

МОНИТОРИНГ В КИИ

- Явно требуется только на значимых объектах

(на незначимых объектах – только оповещение ГОССОПКА по факту атаки)

- ИТ-инфраструктура и АСУ ТП

(В ЗОКИИ существенный мониторинг только в ИТ-инфраструктуре и АСУ ТП)

- Специфика мониторинга автоматизации

(индивидуальный подход сбора событий с оборудования и датчиков)

- Крайности в оснащении оборудованием

(либо модернизированное современное, либо очень древнее – сложное)

- Во главе обеспечение деятельности, а не ИБ

(обеспечение деятельности главное, ИБ как дополнение)

Целевые атаки на КИИ ДФО?

- **Мы никому не нужны.** КИИ становится «интересным» всё чаще, а если громких дел не так много – то **сколько «тлеет» инцидентов?**
- **У нас нечего «мониторить» и атаковать.** «Офис», сетевое оборудование, системы для АСУ ТП на АРМ, спец. оборудование;
- **АСУ ТП – это закрытые системы.** Тренд на централизацию, управление/облегчение манипуляций, мониторинг состояния, каналы связи не свои – а операторы связи неидеальны;
- **А если цель не конфиденциальность – остановка деятельности?** Для вымогательства или просто злонамеренная деятельность.

Таргетированные атаки

- Всегда есть **ЦЕЛИ** – объект или действие
- **Начало** из стандартных атак **«белый шум»** или конкретная **организация**
- Всегда есть **подготовка**
- Это **процесс** распределенный **во времени**

Таргетированные атаки - состав

Подготовка

- анализ цели
- подготовка стратегии
- создание/покупка тулсета

Проникновение

- использование слабых мест
- проникновение внутрь инфраструктуры

Закрепление

- кража идентификационных данных
- повышение привилегий
- налаживание связей
- легитимация действий
- получение контроля

Воздействие

- непосредственно воздействие, кража, шифрование
- сокрытие следов
- создание бэкдоров

ИНСТРУМЕНТЫ мониторинга событий ИБ

- **Классика** – СЗИ, сбор логов с инфраструктуры
- **SIEM-системы** – консолидация, обработка и анализ, категоризация..
- **IDS или IPS** – анализ сетевого трафика
- **Дополнения: TIP или TI Platform, Honeypot, SOAR-системы, EDR или DLP-системы**

ИНСТРУМЕНТЫ мониторинга событий ИБ Дополнительные системы для эффективности

- **TIP** или TI Platform – это средство обработки входящего Threat Intelligence (основное: перечни IOC – IP, FQDN, хэшей и т.д., считающихся злонамеренными) цель – сокращение разрыва между первым обнаружением атаки где-то в мире и возможностью выявлять её в инфраструктуре.

ИНСТРУМЕНТЫ мониторинга событий ИБ Дополнительные системы для эффективности

- **Honeypot** – служит приманкой для сбора информации о злоумышленнике и целевой защиты инфраструктуры; это имитация инфраструктурных объектов

ИНСТРУМЕНТЫ мониторинга событий ИБ Дополнительные системы для эффективности

- **SOAR-системы** – частичная автоматизация действий службы ИБ, алгоритмизация противодействия атакам

ИНСТРУМЕНТЫ мониторинга событий ИБ Дополнительные системы для эффективности

- **DLP-система,** Data Loss Prevention – область специализации: пользователи и их компьютеры; логирование действий и процессов на автоматизированном рабочем месте

Тренды таргетированных атак

- Социальная инженерия как точка входа
- Уязвимость из-за «удаленки», работы персонала вне офиса
- Активизация «шифровальщиков», потеря доступа к данным, шантаж с целью выкупа

Благодарю за внимание!

Вячеслав Ким

заместитель генерального директора

ООО «Информационный центр»

(423) 240-48-66 доб. 7007

E-mail: kim.vs@ic-dv.ru