Уязвимость нулевого дня

НКАбд-01-23

Улитина Мария Максимовна

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Целью данного доклада является изучение информации об уязвимости нулевого дня, рисках данной уязвимости и способах её предотвращения. В данной работе я детально рассмотрю вышеперечисленные аспекты и проиллюстрирую их примерами.

2 Введение

Специалисты сферы информационной безопасности ежедневно сталкиваются с различными типами уязвимостей и угроз. Одной из основных задач в данной области является обнаружение потенциальных угроз безопасности и стабильности быстрее злоумышленников для предотвращения утечек данных и других негативных последствий.

3 Основные понятия

Уязвимость нулевого дня – программная уязвимость, обнаруженная злоумышленниками до того, как о ней узнали производители программы или уязвимость, против которой пока что нет защитных механизмов.

Эксплойт нулевого дня – это метод, используемый злоумышленниками для атаки на системы с не выявленными ранее уязвимостями.

4 Обнаружение уязвимости нулевого дня

Многие предприятия формируют специальные команды для обнаружения уязвимостей нулевго дня. Специалисты в таких отделах могут использоать различные методы в своей работе.

1. Использование существующих баз вредоносных программ. Уже описанные поведения и паттерны могут послужить справочным материалом для обнаружения уязвимостей.

2. Поиск признаков взаимодействия вредоносных программ и возможностей их работы.

3. Применение ИИ и машинного обучения.

5 Опасность уязвимостей нулевого дня

Данные атаки крайне затруднительно предотвратить. При обнаружении уязвимости нулевого дня требуется действовать незамедлительно, чтобы минимизировать потенциальный ущерб.

Атакам нулевого дня подвержены следующие объекты:

1. Операционные системы
2. Браузеры
3. Приложения
4. Интернет вещей
5. Аппаратное обеспечение и прошивка

6 Защита от атак нулевого дня

Для предотвращения атак нулевого дня следует придерживаться определенных правил информационной безопасности.

1. Обновление программ и операционных систем. Производители ПО включают в обновленные версии программ защиту от обнаруженных уязвимостей, обеспечивают соответствие программ современным стандартам безопасности.

2. Использование только необходимого ПО. Чем больше программ применяются, тем больше потенциальная площадь атаки для злоумышленников.

3. Использование сетевого экрана. При правильной настройке сетевой экран вносит огромный вклад в обеспечение безопасности.

4. Обучение персонала. Иногда атаки нулевого дня происходят из-за ошибки сотрудников. При наличии релевантных навыков и знаний сотрудник сможет обеспечить безопасность не только своего рабочего ПК, но и не подставит под угрозы свою организацию.

5. Использование комплексного антивирусного ПО. На данный момент на рынке присутствует огромное количество современного ПО, обеспечивающего защиту от угроз нулевого дня.

7 Выводы

В данном докладе я рассмотрела основные аспекты уязвимостей нулевого дня, а также способы их предотвращения.

Список литературы

1. Что такое атака нулевого дня? Определение и описание от kaspersky
2. Zero Day уязвимость: что такое уязвимость нулевого дня от Solar