В чем преимущества DevSecOps и как обосновать его необходимость бизнесу?

Константин Саматов, член Правления Ассоциации руководителей служб информационной безопасности

Преимущества DevSecOps

- ускорение разработки и внедрения ПО;
- снижение количества случаев возврата кода на доработку;
- снижение стоимости/затратности разработки;
- уменьшение уязвимостей и уменьшение срока их устранения;
- повышение устойчивости к компьютерным атакам;
- снижение вероятности возникновения инцидентов;
- возможность обеспечить приоритет встроенных средств защиты над наложенными.

Кому нужен DevSecOps?

1. Разработчики ПО
2. Субъект КИИ имеющий ЗОКИИ (с 01.01.2023)
3. Владелец ИСПДн с «внешними» пользователями
4. Владелец ГИС и МИС
5. Финансовые организации

Драйверы внедрения в организации

Требования регуляторов

Риски: убытков, деловой репутации, санкций

Инциденты

Повышение эффективности бизнеса

Требования регуляторов

1

Требования Банка России: 382-П, 683-П, 684-П, 719-П:

- Анализ и устранение уязвимостей ПО
- Соответствие ОУД или сертификация

2

П. 11 Состава и содержания… (21 Пр. ФСТЭК России). В случае определения в соответствии с Требованиями к защите ПДн (ПП №1119), в качестве актуальных угроз безопасности персональных данных 1-го и 2-го типов дополнительно **могут применяться** следующие меры:

- проверка системного и (или) прикладного программного обеспечения, включая программный код, на отсутствие недекларированных возможностей с использованием автоматизированных средств и (или) без использования таковых;
- тестирование информационной системы на проникновения;
- использование в информационной системе системного и (или) прикладного программного обеспечения, разработанного с использованием методов защищенного программирования.

Требования регуляторов

3

Требования к владельцам ЗОКИИ. С 01.01.2023 дополняются п. 29.3 - 29.4 (Приказ ФСТЭК России от 20.02.2020 № 35):

29.3. Прикладное ПО, планируемое к внедрению в рамках создания (модернизации или реконструкции, ремонта) ЗОКИИ должно соответствовать:

- требованиям по безопасной разработке: наличие руководства по безопасной разработке программного обеспечения, проведение анализа угроз безопасности информации программного обеспечения, наличие описания структуры программного обеспечения на уровне подсистем;
- требованиям к испытаниям по выявлению уязвимостей в программном обеспечении: SAST, DAST, Fuzzing
- требованиям к поддержке безопасности программного обеспечения: отслеживание и исправление ошибок и уязвимостей, доведение разработчиком информации до его пользователей об уязвимостях и способах получения обновлений, окончании производства и/или поддержки ПО.

Требования регуляторов

3

29.4. Выполнение требований 29.3 оценивается лицом, выполняющим работы по созданию (модернизации, реконструкции, ремонту) или обеспечению безопасности ЗОКИИ, на этапе проектирования на основе документации разработчика ПО.

Риски/Инциденты

1. Успешная КА на крупнейшего мировой производитель алюминия Norsk Hydro - ущерб от инцидента составил порядка $35-41 млн.

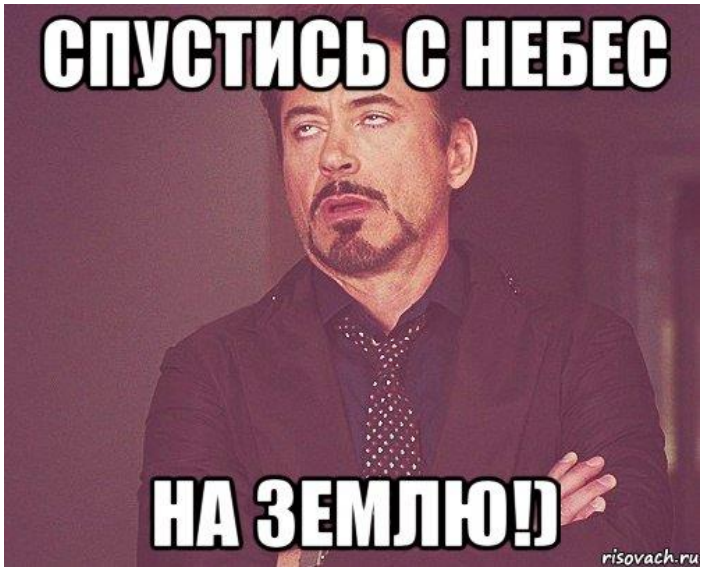
2. Южнокорейская криптовалютная биржа Bithumb - $20 млн., криптовалютная биржа Binance – $41 млн. Кроме того, хищение злоумышленниками большого массива персональной информации трейдеров, секретные ключи, пароли двухфакторной аутентификации и прочие данные.

3. В ходе КА на поставщика облачных сервисов Blackbaud в сети компании был запущен шифровальщик и похищены данные клиентов. Компания заплатила выкуп и надеялась, что злоумышленники не воспользуются украденной информацией. В связи с произошедшим инцидентом компании Blackbaud предъявлено 23 коллективных иска с обвинениями в причинении ущерба.

Риски/Инциденты

4

После того как стало известно об атаке на SolarWinds ее акции за неделю обрушились в цене на 40%, и до сих пор котировки не вернулись к прежнему уровню. Также, в результате атаки на клиентов SolarWinds злоумышленники украли программное обеспечение для проведения тестов на проникновение компании FireEye, которое может быть использовано в новых атаках в ближайшее время.



Экономическая эффективность

- Return on Investment – ROI
- Payback Period – PP
- Benchmarking
- Анализ рынка и обоснование повышения конкурентоспособности
- Value

$$ROI = \frac{EBIT(1-H)}{(C_a^H - C_a^k):2}$$

Спасибо за внимание!

Константин Саматов, член Правления Ассоциации руководителей служб информационной безопасности