О чём могут забыть даже самые внимательные котики?

Анастасия Гайнетдинова,
IT Security Analyst, Whoosh

WHOOSH

Забыть можно о...

- ...ошибках в коде
- ...проверке контрагентов
- ...документации
- ...моделировании угроз

Код и ошибки

Предусловия

- Код нужно написать быстро, потому что фича нужна была вчера.

Код и ошибки

Предусловия

- Код нужно написать быстро, потому что фича нужна была вчера.

Проблема

1. Котик утаскивает код на свой гитхаб (не всегда вспоминая про настройки видимости), чтобы доделать в свободное от работы время.
2. Для дебага котики выводят коды и суть ошибок, на релизе это забывают привести в нормальный вид.
3. Для быстрых тестов в рабочий код зашивают токены доступа.

Код и ошибки

Предусловия

- Код нужно написать быстро, потому что фича нужна была вчера.

Проблема

1. Котик утаскивает код на свой гитхаб (не всегда вспоминая про настройки видимости), чтобы доделать в свободное от работы время.
2. Для дебага котики выводят коды и суть ошибок, на релизе это забывают привести в нормальный вид.
3. Для быстрых тестов в рабочий код зашивают токены доступа.

Последствия

1. Исходники вашего приложения становятся всеобщим достоянием.
2. Перебирая ошибки, которое отдает приложение, злоумышленник подбирает логику работы вашего приложения и векторы атак.
3. Пабаам!

Код и ошибки

Предусловия

- Код нужно написать быстро, потому что фича нужна была вчера.

Выводы

- Триада “быстро-дешево-качественно”.
- SCA/SAST/DAST поможет найти явные ошибки.
- Постройте вашим котикам безопасный удаленный доступ и объясните, к чему ведет нарушение.

Проблема

1. Котик утаскивает код на свой гитхаб (не всегда вспоминая про настройки видимости), чтобы доделать в свободное от работы время.
2. Для дебага котики выводят коды и суть ошибок, на релизе это забывают привести в нормальный вид.
3. Для быстрых тестов в рабочий код зашивают токены доступа.

Последствия

1. Исходники вашего приложения становятся всеобщим достоянием.
2. Перебирая ошибки, которое отдает приложение, злоумышленник подбирает логику работы вашего приложения и векторы атак.
3. Пабаам!

Проверка контрагентов

Предусловия

- Договоры с контрагентами (особенно на поставку сервисов ИБ).

Проверка контрагентов

Предусловия

- Договоры с контрагентами (особенно на поставку сервисов ИБ).

Проблема

1. Проверка только бумажного соответствия
2. Не трожь, пока работает

Проверка контрагентов

Предусловия

- Договоры с контрагентами (особенно на поставку сервисов ИБ).

Проблема

1. Проверка только бумажного соответствия
2. Не трожь, пока работает

Последствия

1. На словах – он Лев Толстой, а на деле может не выдержать нагрузки/атаки

Проверка контрагентов

Предусловия

- Договоры с контрагентами (особенно на поставку сервисов ИБ).

Выводы

- Личное знакомство может сильно помочь в составлении представления о реальном положении дел.
- Не верьте на слово – тестируйте. Желательно, периодически.

Проблема

1. Проверка только бумажного соответствия
2. Не трожь, пока работает

Последствия

1. На словах – он Лев Толстой, а на деле может не выдержать нагрузки/атаки

Документация

Предусловия

- Процессы ИБ в любом состоянии.
- Подразделение ИБ – практики, им не до бумажек.

Документация

Предусловия

- Процессы ИБ в любом состоянии.
- Подразделение ИБ – практики, им не до бумажек.

Проблема

1. Инцидент редко затрагивает только подразделение ИБ. А реагировать нужно всем. Но инструкций нет.
2. Процессы часто сложные и неочевидные. Если некому “на словах” передать новым коллегам, как это обычно работает, есть шанс выстрелить себе же в ногу.

Документация

Предусловия

- Процессы ИБ в любом состоянии.
- Подразделение ИБ – практики, им не до бумажек.

Проблема

1. Инцидент редко затрагивает только подразделение ИБ. А реагировать нужно всем. Но инструкций нет.
2. Процессы часто сложные и неочевидные. Если некому “на словах” передать новым коллегам, как это обычно работает, есть шанс выстрелить себе же в ногу.

Последствия

1. Без четких инструкций, понятных всем, во время инцидента, часть коллег будет бегать по кругу с громкими криками “А-А-А!”.
2. Процессы замыкаются на тех людей, кто уже уже давно работает, и искусственно создается “бутылочное горлышко”.

Документация

Предусловия

- Процессы ИБ в любом состоянии.
- Подразделение ИБ – практики, им не до бумажек.

Проблема

1. Инцидент редко затрагивает только подразделение ИБ. А реагировать нужно всем. Но инструкций нет.
2. Процессы часто сложные и неочевидные. Если некому “на словах” передать новым коллегам, как это обычно работает, есть шанс выстрелить себе же в ногу.

Выводы

- Плэйбуки – не универсальное средство, но они помогут покрыть большую часть частых кейсов.
- Бумага != бумажная безопасность. Иногда это просто эффективный способ распределить нагрузку и обязанности в критичный момент.
- Пропишите обязательные триггеры.
- Подготовьте коллег к возможным последствиям.

Последствия

1. Без четких инструкций, понятных всем, во время инцидента, часть коллег будет бегать по кругу с громкими криками “А-А-А!”.
2. Процессы замыкаются на тех людей, кто уже уже давно работает, и искусственно создается “бутылочное горлышко”.

Нас не заденет

Предусловия

- Бизнес, который ещё не дорос до крупного.
- Отдел ИБ, уверенный, что их компании не привлекательна для злоумышленников.

Нас не заденет

Предусловия

- Бизнес, который ещё не дорос до крупного.
- Отдел ИБ, уверенный, что их компании не привлекательна для злоумышленников.

Проблема

1. Таргетные атаки – не редкость, но и не правило. Массовые атаки на “авось прокатит” за последние 1,5 года стали явлением почти обычным.
2. Никакой злоумышленник не станет отпускать жертву, потому что бизнес небольшой.
3. Любая компания поддерживает контакт с внешним миром, хотябы через почту.

Нас не заденет

Предусловия

- Бизнес, который ещё не дорос до крупного.
- Отдел ИБ, уверенный, что их компании не привлекательна для злоумышленников.

Проблема

1. Таргетные атаки – не редкость, но и не правило. Массовые атаки на “авось прокатит” за последние 1,5 года стали явлением почти обычным.
2. Никакой злоумышленник не станет отпускать жертву, потому что бизнес небольшой.
3. Любая компания поддерживает контакт с внешним миром, хотябы через почту.

Последствия

1. Задеть может кого угодно и когда угодно. Фишинг – отличный способ начать атаку.
2. Даже если вы поставили продвинутые эшелоны защиты, могут остаться открытыми банальные векторы атак.
3. Человек – всегда самое слабое звено в любой системе защиты.

Нас не заденет

Предусловия

- Бизнес, который ещё не дорос до крупного.
- Отдел ИБ, уверенный, что их компании не привлекательна для злоумышленников.

Выводы

- Смиритесь, вас может задеть случайно.
- Не игнорируйте конкурентную борьбу – она не всегда ведется честно, и последствия могут быть очень неожиданными.
- Прежде, чем переходить к сложным системам защиты, убедитесь в работоспособности простых.
- Модель угроз никому ещё не вредила (если у вас её не украли).

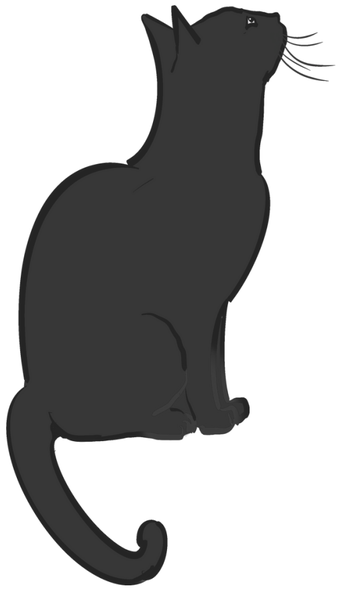
Проблема

1. Таргетные атаки – не редкость, но и не правило. Массовые атаки на “авось прокатит” за последние 1,5 года стали явлением почти обычным.
2. Никакой злоумышленник не станет отпускать жертву, потому что бизнес небольшой.
3. Любая компания поддерживает контакт с внешним миром, хотябы через почту.

Последствия

1. Задеть может кого угодно и когда угодно. Фишинг – отличный способ начать атаку.
2. Даже если вы поставили продвинутые эшелоны защиты, могут остаться открытыми банальные векторы атак.
3. Человек – всегда самое слабое звено в любой системе защиты.

Давайте жить дружно!



Остались вопросы?

Анастасия Гайнетдинова

IT Security Analyst
Whoosh

+7 (999) 466 82 24