Подготовка 1

Установить контакты, выработать процедуры, собрать необходимую информацию для оптимизации временных затрат в момент инцидента.

■ Создать инвентарь всех торговых марок, принадлежащих компании и ее филиалам. Это поможет правильно оценить ситуацию и предотвратить запуск необязательных действий по возвращению прав на истекшую торговую марку, доменное имя или учетную запись в социальных сетях.

■ Создать базу объективных доказательств юридической принадлежности торговых марок вашей компании:
-Марки, легитимные доменные имена, названия учетных записей, используемые вашей компанией и ее филиалами с указанием географической юрисдикции;
-Защищенные торговые слоганы, символы, знаки, графические объекты;
- Регистрационные номера торговых марок;
- Названия международных и национальных организаций (ФГУ ФИПС, Роспатент, USPTO, INPI, и др.), зарегистрировавших ваши торговые марки.
- Иные документы, четко определяющие принадлежность торговых марок вашей организации.

■ Заранее приготовить формуляры абуз-оповещений для заполнения и рассылки заинтересованным сторонам (хостинг провайдеры, регистраторы, вебмэйл провайдеры, социальные сети и т.п.) в момент инцидента. Желательно подготовить формуляры на нескольких языках. Минимально: на языке страны основной операционной деятельности компании и на английском языке.

■ Регистрировать домены компании централизованным образом, используя стандартизованный наименования в WHOIS формах.

■ Придерживаться этических принципов использования Интернет рекламы во избежание появления ваших торговых марок на доменных паркинг-порталах.

Контакты

■ Создать внутренний список лиц, ответственных за регистрацию торговых марок, включая представителей юридического отдела и отдела по связям с общественностью.

■ Создать список лиц, уполномоченных принимать решения по делам нарушения прав использования торговых марок. По возможности, заручится письменным свидетельством полномочий на принятие таких решений для вашей команды.

■ Создать список внешних контактов для использования в рамках реагирования на случаи нарушения прав использования торговых марок.

Подготовка 2

Обнаружить инцидент, определить затрагиваемый периметр, привлечь к решению компетентные стороны.

Нарушения прав использования торговых марок

■ Развернуть процедуры мониторинга регистрации доменных имен. Возможно использования сервисов DomainTools, PremiumDrops и zone-file репозиториев отдельных ccTLD;

■ Настроить работу по мониторингу учетных записей, страниц и групп в социальных сетях;

■ Подвергать регулярному анализу HTTP referrers и логии ваших сайтов; это поможет обнаружить вредоносный контент и незаконное использования текста и графики;

■ Настроить мониторинг использования ваших торговых марок, используя специализированные поисковые сервисы.

По возможности, автоматизировать вышеизложенные процедуры для минимизации временных затрат и человеческих ресурсов на выявление, оповещение и реагирование на инциденты.

Привлечь компетентные стороны

Оповестить сотрудников вашей компании, принимающих решение по данному типу инцидентов. Решения по случаям незаконного использования торговых марок должны приниматься в кратчайшие сроки.

Собрать доказательства

■ Собрать доказательную базу по нарушениям прав использования торговых марок в рамках регистрации доменных имен, создания вебсайтов, групп в социальных сетях, блогов, учетных записей и т.д.

■ Создать датированную копию ресурса-нарушителя. Возможно использование HTTrack. При необходимости сделать копии экранов страниц.

Сдерживание 3

Минимизировать эффект от незаконного использования торговой марки

■ Оценить эффект от нарушения прав использования торговой марки:

- Может ли ресурс быть использован для незаконного перенаправления траффика (кибersквоттинг, черный-SEO)?
- Может ли он быть использован для незаконной подмены, мошеннических операций, подлога (например кибersквоттинг с целью перенаправления на легитимный сайт компании, почтовый домен-легитимизатор для отправки сообщений от лица компании третьими лицами и др.)?
- Возможно ли использование ресурса с целью дискредитации компании или ее брендов?

■ Оценить весомость нарушающих права компонентов:
- Видимость сайта (ranking).
- Количество членов социальной группы, количество «друзей», «followers», « likes » в социальных сетях.

■ Настроить процесс мониторинга зафиксированных неактивных ресурсов с целью своевременного обнаружения вредоносной активности.

- Рекомендуется автоматизировать процесс регулярного наблюдения за подозрительными ресурсами с возможностью мгновенного оповещения причастных лиц в случае изменения контента. Возможно использование Website Watcher или собственных скриптов мониторинга доступности веб-ресурсов.
- - Также, см. IRM-13-Phishing и IRM-14-Scam для дальнейшей информации.

Устранение 4

Устранить угрозу

В большинстве вопросов, связанных с использованием товарных знаков достаточно грамотной организации процесса мониторинга. Переход к активным мерам по устранению проблемы рекомендуется только в случае серьезного негативного эффекта от нарушения прав использования торговой марки.

Доменное имя

- Оповестить владельца и хостинг провайдера домена о факте нарушения прав использования торговой марки; попросить удалить нарушающий права контент.
- Оповестить регистратора доменного имени о нарушении прав использования торговой марки в рамках регистрации домена; попросить заблокировать доменное имя.
- Запросить владельца, регистратора или DNS оператора доменного имени заменить существующие DNS записи на ваши.
- В случае неудовлетворения ваших ходатайств владельцем или регистратором доменного имени, начать процедуру разрешения споров о доменных именах (UDRP) или иную официальную процедуру – в зависимости от типа доменного имени.

Учетная запись в социальной сети

- Связаться с администрацией соцсети, разместившей контент, нарушающий права вашей организации и уведомить их о нарушении политик использования Trademark Policies или Terms of Service, попросив заблокировать причастную учетную запись, группу, контент и т.д.
- По возможности, попросить передать права по администрированию нарушающего ресурса вашей компании.

В качестве формы жалоб, используйте стандартные существующие формы по вопросам abuse, правовых вопросов, вопросам нарушения интеллектуальных прав.

Восстановление 5

Вернуться к нормальному режиму работы

Удостовериться в успешном разрешении проблемы

Убедиться в том, что нарушающий ваши права объект недоступен или перенаправлен под контроль вашей компании.

- Продолжать наблюдение за ресурсом-нарушителем для своевременного обнаружения в случае возвращения вредоносного контента.
- Зарегистрировать освобожденное доменное имя, нарушавшее права использования ваших торговых марок.

После инцидента 6

Задокументировать детали инцидента, обсудить извлеченные уроки, оптимизировать процессы защиты и реагирования.

- Включение каких дополнительных шагов в подготовительную фазу позволит быстрее и эффективнее реагировать на будущие инциденты?
- Обновить список контактов, добавить примечания по оптимизации подхода к каждому контакту.
- Установление каких дополнительных внутренних и внешних контактов поможет увеличить эффективность работы по данному типу инцидентов.
- Взаимодействовать с юридическим отделом в случае подачи официальных жалоб.

SOCIETE GENERALE | CERT SOCIETE GENERALE

Incident Response Methodology

cert.sg@socgen.com / cert.societegenerale.com / @certsg

IRM #15

Незаконное использование торговой марки

Руководящие принципы реагирования на нарушения прав использования товарных знаков

Автор IRM: CERT SG
Версия IRM: 1.1 (RU)

Об IRM

Данная методология по реагированию на инциденты ИБ является кратким руководством, предназначенным вниманию специалистов, работающих над проблемами безопасности:

- Системные администраторы
- Члены Security Operation Centers
- Начальники и представители отделов ИБ
- Представители CERT/CSIRT/IRT

Распространение IRM возможно в рамках SG Group.

В случае обнаружения признаков инцидента, следуйте рекомендациям IRM, делайте заметки, не поддавайтесь панике и немедленно оповестите свой CERT.

Фазы управления инцидентами ИБ

Шесть фаз управления инцидентами ИБ:

- **Подготовка**: подготовится к управлению инцидентом
- **Обнаружение**: идентифицировать проблему
- **Сдерживание**: ограничить негативный эффект
- **Устранение**: ликвидировать угрозу
- **Восстановление**: восстановить до нормального
- **После инцидента**: формализация и совершенствование процесса управления инцидентом

IRM предоставляет детальную информацию по каждой из фаз.

Документ для публичного использования