кабинеты. Особое внимание уделяется защищенности серверов. Также отслеживается любая деятельность через крупные поисковики (определенные запросы), социальные сети, мессенджеры, известные порталы. Google, YouTube, Facebook, Skype и прочие подобные сервисы также представляют потенциальную опасность. Преступниками непрерывно ведется мониторинг деятельности лидирующих компаний в сфере IT (Microsoft, Apple), поскольку выявленные уязвимости помогают им обходить защиту. Вероятность нападения пропорционально увеличивается по мере возрастания популярности соответствующего сервиса и организации.

5.2. Кибеpразведка и контрразведка: цели, задачи, методы работы

5.2.1. Общая информация о кибеpразведке

Кибеpразведка – это разведка, целью которой является информационная безопасность. По определению Gartner, это «основанные на фактических данных знания о существующей или возникающей угрозе или опасности...». По сути, кибеpразведка дает возможность владеть информацией, для того чтобы быть осведомленным о потенциальной вредоносной активности и иметь возможность принимать лучшие решения о том, как предотвратить негативное влияние той или иной угрозы.

Существует три «типа» кибеpразведки:

- стратегическая;
- оперативная;
- тактическая.

Strategic Cyber Intelligence (англ. стратегическая кибеpразведка) (в широком смысле) – это деятельность, направленная на получение информации о современных направлениях развития угроз в сфере информационных технологий. Заниматься этой деятельностью необходимо для предотвращения негативного влияние этих угроз (потеря прибыли, ухудшение репутации и т.д.).

Основными целями стратегической разведки является оценка текущих и снижение будущих рисков. Например, с помощью кибеpразведки корпорация, выпускающая новый продукт или завершающая слияние, сможет оценить не только потенциальное влияние этого действия, но и связанные с этим риски. Это особенно важно для исполнительного руководства, которое должно принимать обоснованные инвестиционные решения.

Оперативная кибеpразведка позволяет специалистам по информационной безопасности выявлять закономерности в атаках, на основе которых могут быть разработаны правила, с помощью которых затем можно будет обнаруживать определенные индикаторы вредоносной активности.

Тактическая кибеpразведка предоставляет аналитикам возможность получать справочный материал для интерпретации и извлечения контекста для использования в оборонительных целях. Эти сведения поступают в виде IOCs, которые включают такие элементы, как домены или IP-адреса. Однако в большинстве случаев показатели быстро меняются, а это означает, что результаты оперативной и стратегической разведки также должны учитываться при принятии решений.

Сочетание этих «типов» кибер разведки помогает специалистам по информационной безопасности предотвращать или оперативно реагировать на возникающие угрозы.

Этапы ведения кибер разведки

Можно выделить 3 основных этапа ведения кибер разведки:

- сбор и аккумуляция данных;
- обогащение полученных данных;
- анализ данных.

Сбор и аккумуляция данных

Сбор данных об угрозах производится с использованием следующих систем:

- поисковые роботы – системы для сбора информации о существующих сайтах в Интернете;
- песочница – изолированная среда для безопасного исполнения подозрительного кода с целью обнаружения и анализа вредоносных программ;
- мониторинг ботнет-сетей – сетей компьютеров под контролем управляющего сервера злоумышленника;
- honeypot – выделенный для злоумышленника в качестве приманки сегмент сети, отделенный от основной защищенной сети организации;
- сенсоры – программы-агенты, собирающие полезную информацию с различных устройств.

Также база данных пополняется базами утечек – чувствительной информацией, попавшей в открытые источники нелегитимным путем. Это могут быть учетные данные от систем и сервисов, адреса электронной почты, данные о кредитных картах, пароли.

Из открытых источников OSINT приходят фиды (структурированные проанализированные данные) – данные об IP-адресах и доменах, с которых идет распространение вредоносных файлов, их сэмплы и хэши; списки фишинговых сайтов и почтовые адреса отправителей фишинговых писем; активность C&C (Command & Control) серверов; адреса, с которых идет сканирование сетей в целях инвентаризации и обнаружения версий систем, баннеров сервисов и уязвимостей; IP-адреса, с которых проводятся bruteforce атаки; Yara сигнатуры для обнаружения вредоносного программного обеспечения.

Полезную информацию можно найти на сайтах аналитических центров, CERT и блогах независимых исследователей: обнаруженные уязвимости, правила для их обнаружения, описания расследований.

Аналитики в процессе расследования целевых атак получают сэмплы вредоносных файлов, их хэши, списки IP-адресов, домены, URL, содержащие нелегитимный контент.

Также в систему поступают данные об обнаруженных уязвимостях в программном обеспечении и атаках от партнеров, вендоров, заказчиков.

Осуществляется сбор информации с СЗИ: антивирусы, IDS/IPS, Firewall, Web Application Firewall, средства анализа трафика, средства регистрации событий, системы защиты от несанкционированного доступа и др.

Все собранные данные аккумулируются в рамках единой платформы, которая позволяет обогащать, анализировать и распространять сведения об угрозах.

Обогащение полученных данных

Собранная информация по конкретным угрозам дополняется контекстной информацией – название угрозы, время обнаружения, геолокация, источник угрозы, обстоятельства, цели и мотивы атакующего.

Также на этом этапе происходит обогащение данных – получение дополнительных атрибутов технического характера к уже известным атакам:

- URL;
- IP-адреса;
- домены;
- whois-данные;
- Passive DNS;
- GeoIP – географическая информация об IP-адресе;
- сэмплы вредоносных файлов и их хэши;
- статистическая и поведенческая информация – техники, тактики и процедуры проведения атак.

Анализ данных

На этапе анализа производится объединение событий и атрибутов, относящихся к одной атаке, по следующим признакам: территориальное расположение, временной период, сектор экономики, преступная группировка и др.

Происходит определение связей между различными событиями – корреляция.

При работе с фидами производится выбор источника фидов в зависимости от отраслевой специфики; типов атак, актуальных для определенной компании; наличие атрибутов и IOCs, которые закрывают риски, не закрытые правилами систем защиты. Затем определяется ценность фида и они приоритезируются, опираясь на следующие параметры:

- источники данных фида – возможно, что данный источник является агрегатором данных из OSINT-источников и не предоставляет никакой собственной аналитики;
- актуальность – своевременность и «свежесть» предоставляемых данных. Надо учитывать два параметра: время от момента обнаружения атаки до распространения фида с данными об угрозе должно быть минимальным; источник должен поставлять фиды с частотой, которая обеспечивает актуальность информации об угрозах;
- уникальность – количество данных, не встречающихся в других фидах. Количество собственной аналитики, которую предоставляет фид;
- встречаемость в других источниках. С первого взгляда может показаться, что если атрибут или IOC встречается в фидах от нескольких источников – можно повысить ему уровень доверия. На самом деле какие-то источники фидов могут черпать данные из одного и того же источника, в котором информация может быть не проверена;
- полнота предоставляемого контекста. Насколько хорошо была отсортирована информация, указаны ли цели атаки, сектор экономики, преступная группировка, используемые инструменты, длительность атаки и др.;

- качество (доля ложных срабатываний) правил для СЗИ, основанных на данных от фида;
- полезность данных – применимость данных фида при расследованиях инцидентов;
- формат предоставления данных. Учитывается удобство обработки и автоматизации их загрузки в платформу.

Для классификации данных из фидов используются следующие инструменты:

- теги;
- таксономии – набор библиотек, классифицированных по процессам проведения атаки, распространения угроз, обмена данными и др. Например, ENISA, CSSA, VERIS, Diamond Model, Kill Chain, CIRCL, MISP имеют свои таксономии;
- кластеризация – набор библиотек, классифицированных по статическим признакам угроз и атак. Например, секторы экономики; используемые инструменты и эксплоиты; TTP (Tacticks, Techniques & Procedures), этапы и методы проникновения, эксплуатации и закрепления в системе, основанные на ATT&CK Matrix.

Аналитики выявляют тактики, техники и процедуры атакующих, накладывают данные и события на модель вторжения в систему и строят цепочки реализации атаки. Важно сформировать общий взгляд на атаку с учетом комплексной архитектуры защищаемой системы и связей между компонентами. Учитывается возможность многоступенчатой атаки, которая затронет несколько хостов и уязвимостей.

Применение результатов

На основе проведенной работы осуществляется прогнозирование – выявляются вероятные направления атак, систематизированные с учетом отраслевой специфики, геолокации, временных рамок, возможных инструментов и степени разрушительности последствий. Выявленные угрозы приоритезируются в зависимости от потенциального ущерба при их реализации.

Собранная база знаний используется при написании правил обнаружения атак для СЗИ, оперативном реагировании на угрозы в рамках SOC и расследовании инцидентов.

Специалисты актуализируют модель угроз и производят переоценку рисков в связи с изменившимися условиями.

5.2.2. Стратегическая кибер разведка как способ управление рисками

Для того чтобы управление рисками было эффективным, необходимо, чтобы высшее руководство принимало участие в управлении стратегической кибер разведкой. Примерный список того, что руководство должно определить для успешной кибер разведки:

- приоритетные требования к разведке;
- требования к критической информации;
- требования к информации о дружественных силах.

Стратегическая кибер разведка может помочь определить, какие активы являются относительно более ценными и потенциально более уязвимы. Также с ее

помощью легче принимать решения в отношении смягчения выявленных угроз и уязвимостей.

Чаще всего компании, обладающие достаточными ресурсами, создают свои подразделения, занимающиеся кибербразведкой, а небольшие компании пользуются услугами «провайдеров кибербезопасности».

На практике используется три способа оценки риска.

Оценка угрозы

Обладая глубокими знаниями о противнике, предприятие может оценить риск, который может включать прямые воздействия на организацию или сопутствующий ущерб. Затем организация должна определить, какие стратегические уязвимости угрозы могут использовать для компрометации информационных активов организации, таких как интеллектуальная собственность и IT-инфраструктура. Оценка уязвимости обсуждается в следующем разделе. В сочетании с оценкой угрозы она очерчивает поверхность потенциальной атаки на организацию. Оценивая эти факторы, специалисты по информационной безопасности предоставляют руководителям и риск-менеджерам бесценный инструмент для понимания подверженности фирмы потенциальному инциденту.

Оценка уязвимостей

Чаще всего для оценки уязвимостей при стратегической кибербразведке приглашают экспертов из организации по обеспечению информационной безопасности. Также нередки случаи дружественного сотрудничества между несколькими различными компаниями для достижения общей цели (обнаружения уязвимостей).

Оценка возможного ущерба

Третьей функцией стратегической кибербразведки в оценке рисков является оценка ущерба. Оценка ущерба очень важна, так как ее результат определяет, выгодно ли использовать те или иные средства информационной безопасности. Использование средств информационной безопасности становится невыгодным, когда среднегодовые затраты на них превышают возможный среднегодовой ущерб. Среднегодовой ущерб считается как произведение ожидаемого количества реализации угроз на величину однократного реализация угрозы. В свою очередь, однократная величина угрозы равна произведению доли ресурса, который будет скомпрометирован при реализации угрозы на стоимость ресурса.

Основные источники информации

Официально основными источниками информации при ведении стратегической кибербразведки являются:

- отчеты о региональных ландшафтах киберугроз;
- отчеты об угрозах, адресованных конкретным индустриям (например, gaming);
- годовые отчеты об угрозах и форкасты на следующий год;
- отчеты по специфичным угрозам для конкретного заказчика (обычно компании из Fortune 500 со значительной зависимостью бизнеса от ИТ).

Таким образом, основная цель стратегической кибербразведки – это уменьшение рисков. Стратегическая информация дает возможность максимально эффективно

производить регулярный пересмотр и модернизацию политик и систем информационной безопасности, осознанно отбирать и внедрять методы защиты, которые позволят противостоять угрозам не только сегодняшнего, но и завтрашнего дня.

5.2.3. Основные цели и задачи киберконтрразведки

Обеспечение корпоративной информационной безопасности – это одна из главных задач для любой современной компании. Не только потому, что данные и информация о своих клиентах, пользователях или поставщиках могут быть подвергнуты риску. Конкурентоспособность компании на рынке также может серьезно пострадать в результате потери конфиденциальной внутренней информации.

Обычно руководство компанией считает, что кибератаки против компаний выполняются исключительно «сторонними лицами», которые никак не связаны с компанией, с исключительной целью продать украденную информацию. Но ведь киберпреступник может работать в конкурирующей компании или даже в «курирующем» компанию государственном органе? Нельзя исключать из внимания и такие случаи, когда кибератака нацелена на кражу «целевой» информации, которая напрямую поставит под угрозу стратегические задачи бизнес-модели и даже инвестиционные проекты компании, которая становится жертвой этой атаки.

Именно здесь руководителям компании и их службам безопасности необходимо использовать практику, которая пока не получила широкого распространения, но начинает приобретать все большее значение среди крупных зарубежных компаний: ***киберконтрразведка***.

Что такое киберконтрразведка?

В классическом понимании этого термина ***контрразведка*** в качестве отправной точки имеет очень простой посыл: *если кто-то атакует вашу компанию, то лучшая оборона – это хорошее нападение*. Вот почему вместо ранее широко применявшихся «превентивных» или «реактивных» действий такого рода современные компании предпочитают менять ситуацию, чтобы «поймать» киберпреступника, который еще только начинает делать свои первые шаги в рамках планируемой им атаки.

Перечислим основные методы работы современных корпоративных киберразведчиков [4].

1. ***Специально оставляют «открытые» двери («мышеловка»).*** Компания может оставить «точку доступа», которая внешне выглядит как неактивированная или незащищенная «уязвимость». Таким образом, киберпреступник найдет эту брешь и подумает, что у него будет возможность проникнуть вглубь информационной сети компании и получить необходимую (заказанную «хозяином») информацию.
2. ***Ложная информация.*** Если киберпреступник действительно воспользуется этой «мышеловкой», то конечно же, он сможет получить доступ к некоей конфиденциальной информации. Однако злоумышленник не будет знать, что этот вход был оставлен «открытым» специально, а добытая им информация не является конфиденциальной. Таким образом, служба безопасности компании обманет киберпреступника, позволив ему «найти» фейковые документы.

3. ***Внимательно изучают информацию об атакующем хакере, пока он ворует.*** До тех пор пока киберпреступник думает, что он находится вне поля зрения и имеет доступ к *действительно* конфиденциальной информации, он будет «совать свой нос» куда угодно. Но он при этом не знает, что компания, которую он «атаковал», на самом деле активно наблюдает за ним, получая дополнительную информацию о хакере для того, чтобы разработать и реализовать возможные меры против него.

Недостатки киберконтрразведки

Может показаться, что киберконтрразведка является идеальным решением, чтобы избежать угрозы информационной безопасности предприятия. Но надо признать, что и у нее есть ряд недостатков.

1. ***Не каждая компания может реализовать эффективную киберконтрразведку.*** Если компания планирует действительно осуществлять эффективные мероприятия по киберконтрразведке, то она должна иметь специально подготовленную для этих целей команду высококвалифицированных (и высокооплачиваемых) специалистов. Само собой разумеется, что далеко не каждая компания может «потянуть» это с финансовой точки зрения, поскольку для этой команды необходимо будет приобрести достаточно дорогостоящие соответствующие программные средства.
2. ***Возможность сбоя.*** Если компания решила «поиграть» в киберконтрразведку, то она должна принять правило этой игры: ведь как и в каждой игре, здесь можно и «проиграть». Например, опытный и высококвалифицированный киберпреступник в этом случае может быть и осведомлен о том, что за ним наблюдают, а потому он может «притворяться» там, где его действительно могут отслеживать, но при этом на самом деле использовать совершенно другие точки проникновения. Все точно так же, как и в противостоянии современных контрразведок без приставки «кибер».
3. ***Юридические конфликты.*** Контрразведка — это не только дело «технарей»: порой она может повлечь за собой и нарушение определенных юридических законов, а это уже означает, что любая компания, которая осуществляет киберконтрразведку, может столкнуться с рядом весьма серьезных юридических проблем, и это надо ясно понимать. Поэтому в состав команды технарей-киберконтрразведчиков крупные компании всегда включают высококвалифицированных юристов, которые «просчитывают» различные варианты развития ситуации.
4. ***Дипломатические конфликты.*** В некоторых случаях кибератаки между компаниями возникают тогда, когда они представляют разные страны, но конкурируют друг с другом за один и тот же проект или контракт или на одном и том же сегменте рынка. В этом случае киберконтрразведка может повлечь за собой дипломатическое «столкновение» с правительственными органами той страны, где находится конкурирующая компания-резидент.

Таким образом, компании, которые действительно хотят защитить корпоративную информационную безопасность, должны использовать менее деликатные, но более безопасные методы. Одним из таких примеров является Panda Adaptive

Defense – это решение, которое не только действует проактивно и реактивно, но также помогает остановить несанкционированный доступ и защитить компании от наиболее известных типов нарушений в их информационной безопасности. Благодаря непрерывному мониторингу всех процессов в корпоративной сети, Panda Adaptive Defense способен оставаться на шаг «впереди» киберпреступников, активируя свои защитные системы еще до возникновения потенциально возможной атаки. Решение с опциями расширенной информационной безопасности обеспечивает более высокие уровни защиты без необходимости использования и других более рискованных и «затратных» техник, таких как киберконтрразведка.

5.2.4. Специфические требования к новому поколению специалистов по информационной и кибербезопасности

Одной из основных острых проблем на начало 2020 г. стала комплексная проблема подготовки специалистов по информационной и кибербезопасности. Эту проблему остро почувствовали не только руководители служб, банков и крупных инфраструктурных предприятий, но и руководители компаний, специализирующиеся на разработке программных и аппаратных средств защиты от киберугроз. К новому поколению специалистов, кроме квалификационных требований, профессиональных специфических знаний, сегодня предъявляется ряд требований к их психологическим характеристикам (чертам характера).

Одной из таких важнейших психологический характеристик, которую чаще всего ищут профессионалы в поисках новых талантов для вышеуказанных компаний, стала так называемая проактивность – *упреждающее действие, которое предпринимают сотрудники по отношению к себе или своему окружению*.

Эта черта характера человека становится все более важной для корпоративной информационной безопасности. Проведенный в 2019 г. среди специалистов по ИБ опрос известной консалтинговой компании ESG, показал, что 53% компаний и организаций сообщили о проблеме нехватки знаний и навыков по информационной безопасности у своих сотрудников. Причем в качестве одной из наиболее сложных проблем была отмечена проблема поиска кандидатов, обладающих *проактивным отношением к поиску и прогнозированию угроз, выходя за рамки традиционных подходов по реагированию на кибератаки*. Как говорят эксперты, проактивность – это основной ключ к решению задач Threat Hunting (охоте за угрозами).

Предпочтение именно «охоте за угрозами» предприятия и банки отдают по той причине, что традиционные средства информационной безопасности, такие как фаерволы, системы обнаружения вторжений (IDS), песочницы или рассмотренные нами в SXX, SIEM-решения, как правило, фокусируются на расследованиях *по факту произошедшего инцидента*. Конечно, эти средства по-прежнему актуальны, т.к. организациям все еще требуется реагировать на наиболее распространенные (известные) кибератаки.

Но как было отмечено выше, кибератаки становятся все более скрытыми и сложными и случаются они все чаще и чаще. В 2019 г. эксперты отмечали, что 62% компаний подвергались кибератакам, которые не использовали какие-либо вредоносные программы. Другие примеры, такие как атаки с использованием чат-

ботов, вредоносные маркетинговые техники, а также другие атаки, основанные на искусственном интеллекте, показали, насколько сложными могут быть новые кибератаки. Компании и банки уже хорошо знают об этом, а потому предпринимают соответствующие меры: регулярно проводят такую «охоту за угрозами» (threat hunting) в рамках своей внутренней стратегии по предотвращению киберрисков.

Каким должен быть специалист по Threat Hunting?

Эти новые угрозы также вызвали серьезную эволюцию в профиле (специализации) киберзлоумышленников: хотя мы все еще можем встретить среди них многих *любителей*, тем не менее теперь большинство из них представляют собой *профессионалов* со специализированной подготовкой и огромными ресурсами, которые они получают от «определенных компаний» или даже от ряда государственных органов своих стран. Киберпреступность теперь чрезвычайно *прибыльный и перспективный бизнес*. Поэтому жизненно важно, чтобы специалисты по информационной безопасности были на одном уровне (а лучше – выше) с современными киберпреступниками. Это означает, что им необходимо выходить далеко за рамки традиционных техник, которые они изучали в вузах и осуществлять активный поиск угроз в корпоративных сетях, используя ***подход, основанный на гипотезах и доказательствах***. Поэтому ***проактивность*** – это ключевое качество для хорошего «охотника за угрозами». Но это не единственное качество (требование). Ниже мы пройдемся по характеристикам, которыми должен обладать каждый профессионал по threat hunting [https://www.cloudav.ru/mediacenter/security/threat-hunters-cybersecurity-specialists/].

- ***Технические знания*:** для организации в компании (банке) любого процесса Threat Hunting крайне важно иметь профессионалов, владеющих глубокими знаниями и опытом в сфере информационной безопасности. Они должны знать традиционные инструменты защиты конечных устройств (EPP), а также и новые подходы: например – Endpoint Detection and Response (EDR), который предполагает использование в режиме реального времени инструментов мониторинга, которые крайне необходимы для качественного Threat Hunting.
- ***Корпоративное и геополитическое видение проблем*:** киберзлоумышленники становятся все более профессиональными, иногда даже они уже входят в состав «легализованных» компаний или даже государственных структур. Следовательно, «охотники за угрозами» должны хорошо *знать корпоративный и геополитический контекст*, который может мотивировать кибератаки на защищаемую ими корпорацию (банк, орган госуправления и т.п). Конечно, технические знания имеют фундаментальное значение, но для того чтобы «опережать» возможные кибератаки, необходимо теперь иметь еще и идеи, которые позволяют иметь более полное представление обо всех процессах, тенденциях, разнообразных сценариях и моделях развития атак и т.д.
- ***Креативность:*** *первый шаг в процессе Threat Hunting* – это *создание гипотез* для поиска потенциальных угроз. Следовательно, «охотник за угрозами» должен сам придумать (написать) возможные сценарии с учетом многочисленных элементов и векторов атак, которые в большинстве случаев могут быть не столь очевидны для традиционных решений кибербезопасности.