АЛЕКСЕЙ ЛУКАЦКИЙ,
бизнес-консультант
по безопасности Cisco

Фонарь как отражение состояния современной ИБ

Сто лет назад Александр Блок написал одно из своих известных стихотворений, которое настолько прочно засело у меня в голове после школьных уроков литературы, что регулярно всплывает, к месту и не очень:

> Ночь, улица, фонарь, аптека,
> Бессмысленный и тусклый свет.
> Живи еще хоть четверть века —
> Всё будет так. Исхода нет.

Вот и сейчас, находясь в нашем кампусе в Калифорнии, я облокотился на современный фонарь и задумался о том, насколько все изменилось в области информационной безопасности за последние годы. И фонарь, как ничто другое, хорошо иллюстрирует эти изменения, которые неявно и постепенно, но заставили совершенно по-другому взглянуть на привычные действия служб, ранее охранявших конфиденциальную информацию от преступных посягательств хакеров.

Что представляет собой фонарь, установленный в нашем кампусе, с точки зрения современных технологий? Это просто кишащее различными сенсорами и датчиками устройство, подключенное к нашей корпоративной сети, раздающее Wi-Fi, обрабатывающее персональные данные (иногда и биометрические) и активно общающееся с Интернетом и различными облачными сервисами. Вроде бы обычный фонарь, а вроде бы и элемент «Интернета вещей». Вроде бы и не сервер с важными данными, и пользователей у фонаря нет, а защиты требует не меньше. Пусть даже мы об этом и не задумываемся. А задумываться надо.

Так сложилось, что я имею некоторое отношение к нашей внутренней службе информационной безопасности и прекрасно по-

нимаю, с какими проблемами сегодня ей приходится сталкиваться. И мне хотелось бы показать, что это за проблемы, на примере именно фонаря из нашего кампуса.

Контроль доступа

Начать защиту фонаря необходимо с четкого определения, куда ему можно подключаться, а куда нет. Особую пикантность этой задаче придает тот факт, что фонарь содержит несколько различных сенсоров, которые передают данные в разные системы, локальные и облачные: сейсмодатчики, датчики дождя и движения, интерком, цифровые вывески и т. п. И из разных систем в фонарь динамически поступают данные, например из систем управления чрезвычайными ситуациями (в громкоговоритель), из службы безопасности (в интерком). А еще через фонарь находящиеся рядом люди могут получить беспроводной доступ к разным участкам корпоративной сети: работники — к внутренним ресурсам, вышедшие покурить гости — только к Интернету. И все это один фонарь, а у нас в кампусе много не только фонарей, но и других интернет-вещей.

Задачу контроля столь разнообразной инфраструктуры пытаться решить в лоб, прописывая правила на каждом инфраструктурном устройстве (точке доступа, коммутаторе или маршрутизаторе) по принципу «узлу А разрешить доступ к узлу Б», можно, но уже на десятом устройстве мы поймем, что погорячились. Это не только займет время на прописывание и проверку списков контроля доступа, но и снизит производительность сетевых устройств, вынужденных проверять каждый пришедший фрейм или пакет на соответствие ACL. А если вспомнить еще про мобильность сотрудников, постоянно находящихся в разных местах корпоративной сети или за ее пределами (и все это в течение одного дня), то задание статических правил не только неэффективно, но и нереально. В конечном итоге все правила превратятся в классическое «всем разрешено всё и всюду», что явно не послужит примером того, к чему стоит стремиться. В итоге мы пришли к контекстной политике доступа, которая опирается не на один атрибут (кто/что), а учитывает множество факторов, отвечающих на следующие вопросы:

- **КТО** подключается?
- **ЧТО** подключается?
- **КАК** осуществляется подключение?
- **ГДЕ** находится подключаемое устройство или пользователь?
- **ОТКУДА** осуществляется доступ?
- **КОГДА** осуществляется доступ?
- **КАКИЕ УСЛОВИЯ** должны быть соблюдены для предоставления доступа?

КТО?	ЧТО?	КАК?
• Известные пользователи (сотрудники, продавцы, HR) • Неизвестные пользователи	• Идентификатор устройства • Классификация устройств (профиль) • Состояние устройства (posture)	• Проводное подключение • Беспроводное подключение • VPN-подключение
ГДЕ/КУДА/ОТКУДА?	**КОГДА?**	**ДРУГИЕ**
• Географическое положение • Департамент/отдел • SSID/ Порт коммутатора	• Дата • Время	• Пользовательские атрибуты • Статус устройства/пользователя • Используемые приложения

Борьба с угрозами

Теперь возьмем вторую распространенную задачу, тоже невольно претерпевшую серьезные изменения. Речь пойдет о борьбе с угрозами, а точнее об источниках получения информации об угрозах. Сколько их у нас? Обычно один — это производители нашего антивируса или системы обнаружения атак, которые регулярно поставляют обновления баз сигнатур для наших продуктов ИБ. Но сейчас такая «однополярность» создает определенные проблемы:

- Необнаружение каких-то угроз (причин этого может быть много).
- Получение информации с ошибками.
- Отсутствие или исчезновение информации на конкретные угрозы.
- Отсутствие учета вертикальной или страновой специфики.
- Смена политики лицензирования:
  - смена собственника;
  - поглощение компании-разработчика;
  - сотрудничество со спецслужбами;
  - санкции.

Начать защиту фонаря необходимо с четкого определения, куда ему можно подключаться, а куда нет

Например, недавно, в ноябре прошлого года, компания Soltra, являющаяся поставщиком сведений об атаках для центра обмена информацией об угрозах в финансовой индустрии США (FS-ISAC), внезапно объявила о прекращении своей деятельности. А регулярные сообщения о том, что тот или иной антивирус не ловит какую-нибудь новомодную угрозу или, что еще хуже, целенаправленную атаку...

Сегодня настало время перестать доверять только одному источнику информации об угрозах. Необходимо получать данные из разных мест — частных компаний и государственных структур (например, ГосСОПКА или FinCERT), платных (в частности, Threat Grid) и свободных (в том числе MalwareDomains.com), принадлежащих известным игрокам рынка (скажем, Facebook) и начинающим стартапам (к примеру, ThreatQ). И чем масштабнее защищаемая сеть, тем больше таких источников понадобится. А для управления ими необходима система, принадлежащая к активно развивающемуся классу решений Threat Intelligence. Тут главное, чтобы используемые источники информации об угрозах поставляли именно для вашей инфраструктуры и ее составных частей, например, «Интернет вещей», которыми напичкан рассматриваемый фонарь в нашем кампусе. При этом стоит обращать внимание на следующие параметры при выборе источника и платформы Threat Intelligence:

- Тип источника.
- Уровни представления информации.

- Широта охвата.
- Число записей.
- Языковая поддержка/покрытие.
- Доверие к источнику (популярность и отзывы).
- Оперативность/частота предоставления информации.
- Формат представления.
- Платность.
- Возможность автоматизации.
- Соответствие вашей инфраструктуре.
- Частота ложных срабатываний.
- Возможность отката назад или пересмотра статуса угрозы (например, для вылеченного сайта).
- Масштаб.
- Удобство использования.
- Гарантии.

В противном случае мы становимся заложниками нашего поставщика антивируса, который может и пропустить какую-то атаку на наш фонарь, и тот превратится в плацдарм для распространения вредоносного кода по внутренней сети или в хранилище украденной информации, на что мы вряд ли обратим внимание, предоставив возможность злоумышленнику долго оставаться незамеченным. Кстати, если быть ближе к российским реалиям, то фонарь можно заменить на принтер, видеокамеру, СКУД или иное устройство, подключенное к внутренней IP-сети, которое обычно выпадает из поля зрения корпоративных или ведомственных служб ИБ.

Мониторинг аномалий

Вернемся к фонарю. Чем он отличается от персонального компьютера, ноутбука или смартфона? Тем, что на него нельзя поставить антивирус или иное средство защиты. Да и от производителя его начинки сложно ожидать, что он будет заботиться о безопасности и внедрять в фонарь механизмы защиты. По крайней мере на этапе завоевания рынка этого обычно не бывает — производители заинтересованы в скорейшем завоевании доли рынка, а не в увеличении времени на разработку и тестирование. Как же поступить в такой ситуации? Как уберечь то, что нельзя защитить?

В пору вспомнить про социальную рекламу «Если человека нельзя вылечить, это не значит, что ему нельзя помочь». С фонарем, как и любым иным IP-устройством, ситуация схожая. Если нельзя поставить средство защиты, то вокруг устройства надо возвести неприступную стену. Эту проблему устраняют системы контроля сетевого доступа, решающие подобные вопросы. Но стена стеной, но даже в них бывают прорехи. Поэтому наша задача заключается в мониторинге происходящего с фонарем и обнаружении следов хакерской или аномальной деятельности. И ту нам на помощь приходит новая технология, ранее не присутствовавшая в шортлисте специалистов по ИБ. Речь идет об обнаружении сетевых аномалий. Данные решения работают по знакомому многим айтишникам принципу — собирают телеметрию NetFlow (или sFlow, cFlow, J-Flow, IPFIX) с имеющегося сетевого оборудования, в том числе с коммутаторов, маршрутизаторов, точек беспроводного доступа (а даже фонарь, подключенный к Интернету, не может миновать этих устройств), и накладывают на них специальные алгоритмы, призванные искать в собранной телеметрии следы несанкционированной деятельности. При ее обнаружении можно дать команду средствам контроля сетевого доступа купировать угрозу, не давая ей распространяться по внутренней сети предприятия. Ведь часто угроза попадает в сеть, минуя периметр и установленные на нем межсетевые экраны и системы предотвращения вторжения. Через точку доступа на фонаре любой гость способен подключиться к внутренней сети и попробовать натворить

Через точку доступа на фонаре любой гость способен подключиться к внутренней сети и попробовать натворить плохих дел

плохих дел. Системы обнаружения аномалий превращают сетевую инфраструктуру в распределенную систему защиты, тем самым сохраняя сделанные инвестиции в сетевое оборудование, которое теперь не только передает трафик из точки А в точку Б, но и занимается его анализом и контролем, в том числе анализируя и трафик от фонаря и других интернет-вещей.

Аналогичную задачу, но уже в Интернете (например, для мобильных устройств) решают системы мониторинга DNS-трафика, который по статистике используется 93% вредоносных программ для скрытия своей активности — загрузки новых модулей и обновлений, получения команд от управляющих серверов, утечки украденной информации. Как мониторить корпоративные устройства, не находящиеся под сенью средств защиты периметра? DNS является, по сути, единственным источником информации, который можно и нужно взять под контроль. И это тоже новая тема, ранее не стоявшая на повестке дня у специалистов по ИБ, привыкших защищать периметр своей сети, а не то, что находится внутри или за ее пределами.

Множество средств защиты

Согласно ежегодному отчету Cisco Annual Cybersecurity Report 2017, 65% компаний используют от 6 до 50 различных средств защиты, превращая свою инфраструктуру безопасности в зоопарк неплохих (а может быть, и лучших), но разрозненных элементов. Специалисты ИТ- и ИБ-служб вынуждены тратить много времени на то, чтобы увязать все компоненты в единый, целостный организм, что получается далеко не всегда. Именно поэтому сегодня на первый план выходит не просто наличие средств обеспечения ИБ на предприятии, а их умение общаться между собой, автоматизируя рутинные задачи и максимально исключая из такого взаимодействия человеческий фактор.

Возьмем, например, историю с кампусом нашей компании в Сан-Хосе, где располагается штаб-квартира. Имеется несколько десятков зданий, разбросанных на территории в несколько десятков квадратных километров. Вы представляете, сколько там умных фонарей? А желающих проникнуть в наши корпоративные тайны? А просто случайных действий, способных нанести нам ущерб? Поэтому так важно, чтобы применяемые или приобретаемые средства защиты обладали набором API, интерфейсов, с помощью которых они могут обмениваться информацией об угрозах, а также давать команды друг другу по блокированию или локализации обнаруженных угроз и аномалий. Когда у нас защита строится на базе антивируса, межсетевого экрана и антиспам-фильтра, то их постоянная ручная настройка и перестройка не составляют большого труда. Но представьте, что у вас несколько десятков типов таких средств, они расположены в сотнях ваших офисов, а сама корпоративная сеть является динамично изменяющимся организмом... Никакая, даже разросшаяся служба ИБ из десятков администраторов безопасности не способна эффективно управлять политикой кибербезопасности. Известный факт: чем больше элементов в системе, тем выше ее сложность и больше вероятность что-то недоглядеть и сделать ошибку. А злоумышленнику как раз и нужно найти всего одну вашу ошибку, чтобы свести на нет все усилия в области защиты информации. Поэтому так важна сегодня автоматизация и открытость средств защиты, которые могут динамически обмениваться данными не только между решениями одного производителя, но и между решениями разных компаний.

В заключение

Возвращаясь к стихотворению поэта, прожившего всю жизнь в Санкт-Петербурге, мне хочется с ним не согласиться. В начале XX века фонарь, действительно, мог стоять на набережной Большой Невки и десять, и двадцать лет, и четверть века и не претерпевать никаких изменений. Сегодня же, в XXI веке, технологии, проникшие во все сферы нашей жизни, заставляют нас по-другому взглянуть на привычные предметы. Взглянуть в том числе и с точки зрения кибербезопасности. Пришла пора перемен.

Революцьонный держите шаг!
Неугомонный не дремлет враг!