Как предотвратить очередное цифровое ограбление

На рубеже XX и XXI столетий в моду вошли фильмы про ограбления. Голливудские знаменитости перевоплощались в гениев преступного мира и совершали чудовищные по масштабам преступления против банков во благо сюжета и на потеху публике. О судьбе вкладчиков тогда мало кто беспокоился, ведь главному герою необходимо было достичь цели

Текст
АНДРЕЙ КУЗНЕЦОВ,
ЭКСПЕРТ «АЙТИ БАСТИОН»



Фото: «АйТи Бастион»

Сейчас времена другие, а главные (анти)герои — повсюду. Если раньше столкнуться с ограблением было чем-то «из ряда вон», то сегодня — суровая обыденность, а для совершения очередного цифрового ограбления нужен разве что доступ в сеть. Для защиты большой инфраструктуры уже не хватает команды «спецов», нужны автоматизированные решения.

Ограбления, утечки данных, обманутые вкладчики и, конечно, старый добрый DDoS: у всех этих страшных вещей много общего, но по-настоящему их объединяет одно — колоссальные средства, затраченные на защиту от них. К сожалению, подобные вложения не всегда оправданы, словно таблетки от кашля, бесполезные против головной боли. Порой даже самые крупные игроки этой системы становятся заложниками подобного подхода (недавний случай утечки у крупного российского банка — пример тому). Чтобы бороться «на той стороне», необходимо правильно расставлять приоритеты в области кибербезопасности и автоматизировать десятки процессов, сведя участие человека в них к максимально допустимому минимуму. Банковская инфраструктура — это синтез тысяч процессов, каждый из которых необходимо регулировать, обновлять, а еще — постоянно мониторить и собирать телеметрию. Отсутствие подобных данных, доступных «здесь и сейчас», чревато большими проблемами, вплоть до потери конкурентоспособности. Сегодня финансовые организации в России — объекты критической информационной инфраструктуры (КИИ), в связи с чем требования регуляторов невероятно высоки.

Из очевидных рисков недостаточной защищенности банка — крупные финансовые потери. А вот несколько неочевидных:

- **утечки** — доступ к базе данных любой организации дает «топливо» для мошенников практически в неограниченных масштабах;
- **остановка бизнес-процессов** — в случае внедрения в цепочку операций вредоносное ПО способно полностью остановить технологический процесс, подвергнув риску не только активы компании, но и деньги вкладчиков;
- **внутренние угрозы** — инсайдеры и дилетанты — два столпа, на которых держится мир кибератак;
- **ограничения** — помимо прочего вреда подтвержденные кибератаки приводят за собой контролирующие органы, а у регуляторов целый арсенал санкций — от штрафов до приостановки лицензии.

Чтобы избежать плачевного исхода и описанных выше рисков, многие прибегают к правильным, но не всегда эффективным мерам. Один из самых верных путей борьбы с уязвимостями — надежная сегментация критических объектов инфраструктуры, вплоть до полной изоляции сетей. Гарантированная изоляция на сегодняшний день достигается за счет использования «воздушного зазора»: его наличие затрудняет необходимый обмен данными и файлами между несвязанными системами. Для связи с закрытыми участками сети часто используется перенос необходимых данных на доверенных съемных носителях (иными словами, флешках). Однако у такого метода передачи существуют весьма серьезные проблемы:

- информация поступает неравномерно, что провоцирует большую задержку в бизнес-процессах;
- рутинность и частое повторение процесса передачи (при записи или проверке накопителя после записи или перед передачей) может заставить совершить ошибку или намеренное игнорирование протокола. Такая «халатность» может повлечь занесение «вредоноса» в изолированный сегмент;
- человеческий фактор может спровоцировать появление ошибок в протоколировании, которые впоследствии вызовут траты большого количества ресурсов на расследование возможного инцидента.

Подобные вещи часто решают путем создания автоматизированных решений, иногда даже самописных: затраты на такие продукты существенно меньше, чем на решения «из коробки». Однако данные средства невозможно или крайне тяжело сертифицировать, что особенно важно для финтеха. К тому же далеко не факт, что эти средства информационного обмена (СИО) будут надежны, ведь, вероятнее всего, созданы они будут специалистами на аутсорсе без специфики под конкретного заказчика.

На фоне этих вводных появился «Синоникс» — система информационного обмена, представляющая собой специальное программное обеспечение в составе программно-аппаратного средства. Основным назначением решения является автоматизация процессов передачи файловой и потоковой информации между сетевыми приложениями. «Синоникс» позволяет построить автоматизированную однонаправленную или двунаправленную передачу данных и файлов между узлами двух сетей, делая их при этом невидимыми.

«Синоникс» основан на использовании технологии автоматизированной электронной передачи информации с применением разрешающих правил, установленных в явном виде. Они обеспечивают безопасный обмен данными и файлами между узлами, в том числе из несвязанных между собой сетей. Решение позволяет практически полностью автоматизировать процесс передачи информации и минимизировать участие человека в нем во избежание компрометации.

Правила задаются на каждом из двух узлов устройства независимо и согласованно для выбранного канала передачи данных и файлов. Если для одного из узлов правила не заданы, то данные переданы не будут. За конфигурацию узла и сегмента отвечает отдельный специалист в своей сети, а определение разрешенного канала передачи данных задается как IP источника, порт для приема пакетов и IP назначения, порт назначения.

«Синоникс» может использоваться совместно с межсетевым экраном (МЭ) и NGFW, а также с другими классами решений. К примеру, возьмем ситуацию, когда из офисного сегмента сети нужно передать файлы (например, обновления) в продуктивный сегмент, не связанный с основным в целях безопасности. Для этого можно использовать «Синоникс» в сочетании с PAM-платформой (Privileged Access Management) СКДПУ НТ.

Такая экосистема обеспечит администраторам удаленный доступ к ключевым ресурсам продуктивного сегмента, позволив передавать файлы обновлений и совершать другие операции по обслуживанию систем. «Синоникс» же, перед тем как передать файлы в несвязанную сеть, будет проводить ряд проверок, заданных администратором, а именно:

- проверка маски файла (формата имени) и его размера;
- контроль целостности файла;
- валидация через внешние системы по протоколу ICAP.

Если все заданные проверки пройдены, то «Синоникс» «пропустит» файл в изолированный сегмент, где он может быть размещен как в собственном файловом хранилище, так и на целевом сервере по протоколам SFTP и FTP.

Сегодняшний финтех нуждается в автоматизированных решениях информационной безопасности, возможно, даже больше, чем раньше. Компании растут, гиганты рынка ежегодно достигают высоких результатов, появляясь в различных рейтингах на лидирующих местах. Однако все это может закончиться, как по щелчку пальца, если не двигаться в ногу со временем, обеспечивая себя современными и работающими продуктами, сценарии применения которых каждый желающий может придумать сам. Б.О

Реклама
АЙТИБАСТИОН
ООО «АиТи Бастион»
Москва, ул. Старовольнская, 15, к.1
+7 (499) 322-36-67
info@it-bastion.com