БАНК САНКТ-ПЕТЕРБУРГ

Обеспечение безопасности и конфиденциальности корпоративной переписки

Название
Банк «Санкт-Петербург»

Отрасль
Финансы

Расположение
Российская Федерация, Санкт-Петербург. Отделения и филиалы на территории Санкт-Петербурга, Ленинградской области, Москвы, Калининграда

Сайт
www.bspb.ru

Кол-во сотрудников
Более 3000 человек

Банк «Санкт-Петербург» внедрил Trend Micro Deep Discovery Email Inspector

ИНФРАСТРУКТУРА

- Два крупных распределенных ЦОД
- Корпоративное облако закрытого типа
- Корпоративная мобильная инфраструктура + BYOD

ПРОБЛЕМА

- Неоднократные сложные атаки, в том числе «нулевого дня», а также класса «компрометация деловой корреспонденции» (BEC)
- Сложность внедрения нового антивирусного ПО
- Необходимость гарантии совместимости с существующей инфраструктурой
- Необходимость обеспечить непрерывность критических для бизнеса процессов при внедрении
- Высокая загрузка ИТ- и ИБ-служб при ручной обработке инцидентов

РЕШЕНИЕ

- Сравнительное тестирование решений от ведущих вендоров
- Выбор продукта Trend Micro Deep Discovery Email Inspector
- Внедрение продукта в существующую ИТ-инфраструктуру
- Настройка ПО для работы в режиме Prevent (автоматическом)

РЕЗУЛЬТАТЫ

- Достигнута 100% совместимость с текущей инфраструктурой
- Внедрение прошло без нарушения критических бизнес-процессов
- С момента внедрения было отражено четыре крупные продолжительные целевые атаки
- Объем ручной обработки инцидентов в отделах ИБ и ИТ значительно сократился
- Сформирован специализированный отдел для разбора инцидентов информационной безопасности

ПРОФИЛЬ КОМПАНИИ

Один из крупнейших региональных банков России — ПАО «Банк «Санкт-Петербург» основан в 1990 году. Банк осуществляет свою деятельность на территории Санкт-Петербурга, Ленинградской области, Москвы, Калининграда.

По результатам ежегодной финансовой отчетности Банк в течение последнего десятилетия демонстрирует устойчивость и стабильность на всех основных рынках финансовых услуг. Приоритетные направления деятельности Банка — кредитование, расчетно-кассовое обслуживание, обслуживание юридических и физических лиц, операции на валютном рынке, рынке межбанковских кредитов, операции с ценными бумагами. Наличие собственного процессингового центра позволяет Банку на высочайшем уровне поддерживать и обслуживать пластиковые карты.

Благодаря правильно избранной стратегии, последовательной финансовой политике, приверженности ценностям цивилизованного ведения бизнеса Банк на протяжении многих лет сохраняет репутацию сильного и надежного партнера.

TREND MICRO DEEP DISCOVERY

Deep Discovery Email Inspector

http://www.trendmicro.com.ru/products/deep-discovery/index.html#email-protection

Решение для защиты электронной почты на основе передовых технологий обнаружения угроз и создания изолированной среды, способных выявлять и блокировать целевые почтовые сообщения с фишинговым содержанием, которые являются предвестниками большинства направленных атак. Оно снижает риск атак, добавляя прозрачный уровень дополнительных проверок, на котором обнаруживаются вредоносный контент, вложения и URL-ссылки, не выявляемые стандартными решениями для защиты электронной почты.

Email Inspector функционирует в сети, взаимодействуя с существующими решениями для защиты почтовых шлюзов и серверов. Продукт поддерживает как режим блокировки угроз, так и режим мониторинга. Для его использования не требуется вносить изменения в политики или схему управления существующими решениями.

«Во время сравнительного тестирования продукт Trend Micro удовлетворил нас по двум самым важным показателям: во-первых, на сравнительных тестах он показал лучшие результаты, а во-вторых, обеспечил полную совместимость с нашим специализированным критическим ПО»

— начальник отдела внедрения и развития технической поддержки средств защиты информации Банка «Санкт-Петербург»
Шуров Денис Александрович

Кейс

ПРОБЛЕМА

Сектор банковских услуг представляет особый интерес для киберпреступников. В последние годы набирают обороты целенаправленные атаки, в рамках которых преступникам зачастую удается похитить из финансовых учреждений значительные суммы денег. Один из самых популярных каналов реализации подобных атак — корпоративная электронная почта. Для банков крайне важно одновременно сохранить оперативность отправки/получения почтовых сообщений и при этом исключить любую возможность их компрометации. Банку «Санкт-Петербург», занимающему 19-е место в рейтинге российских банков, удалось значительно повысить уровень информационной безопасности и оптимизировать рабочие процессы благодаря внедрению Deep Discovery Email Inspector от Trend Micro.

Банк «Санкт-Петербург» входит в число крупных российских банков, общее количество его сотрудников превышает 3000 человек. Профиль деятельности предприятия предполагает высокие объемы электронной корреспонденции. При этом в банке предъявляются особые требования к ИТ-инфраструктуре и средствам ее защиты — расположение вычислительных мощностей и хранимых данных должно быть строго на территории Российской Федерации.

Деятельность банковской организации — непрерывный процесс. Простои и инциденты неприемлемы и могут обернуться утратой доверия к Банку, а также крупными финансовыми потерями. Сложность внедрения любого стороннего ПО также связана со сложностью внутренней ИТ-инфраструктуры предприятия и необходимостью обеспечить совместимость между ее элементами. Помимо этого, система распределена географически — у банка большая сеть офисов и филиалов.

Высокая загрузка службы ИБ обуславливалась большими объемами корреспонденции с партнерами, клиентами, различными государственными органами, которая анализировалась в полуавтоматическом режиме. Также приходилось по косвенным признакам выявлять вторжения и передавать их на локализацию и устранение в службу ИТ. Из-за распределенного характера системы служба информационной безопасности Банка не всегда могла оперативно отреагировать, определить, действительно ли произошло заражение, локализовать проблему и разработать алгоритм дальнейших действий.

РЕШЕНИЕ

Для решения перечисленных проблем в Банке был развернут крупномасштабный пилотный проект по тестированию средств защиты корпоративной переписки. В Банке параллельно были установлены четыре продукта одного класса от разных вендоров. Наблюдения и оценка эффективности и точности работы проводились в реальном времени. Кроме проверки уровня защиты на реальном почтовом трафике Банка, в сообщения подмешивались синтетические образцы, что позволило всесторонне оценить возможности продуктов. Помимо этого, во время очередной итерации пилотного тестирования сотрудники Банка столкнулись с реальной целевой атакой, что позволило сравнить конкурирующие продукты в «боевом» режиме.

Выделенный бюджет позволял выбрать любое из представленных решений, так что отбор шел исключительно по качественным критериям.

По совокупности выявленных угроз и скорости реакции на них решение Trend Micro оказалось лучше других систем. Решающую роль сыграли не только число выявленных угроз и скорость их обнаружения, но и возможность полной совместимости со специализированным критическим ПО Банка.

В целях обеспечения непрерывности критических бизнес-процессов внедрение продлилось четыре месяца. В процессе освоения ПО была отлажена работа системы в режиме с автоматическим распознаванием и блокировкой угроз.

Возникающие во время проекта сопутствующие сложности и вопросы оперативно и грамотно решались при помощи службы технической поддержки Trend Micro. «Техническая поддержка Trend Micro помогла нам настроить продукт под наши специфические требования. Отдельным плюсом является ее локализация. При переписке с иностранной поддержкой всегда есть временной лаг с ответами и определенный языковой барьер, в случае с Trend Micro мы получали оперативные ответы на русском языке, а иногда было даже проще позвонить коротко и проконсультироваться», — отмечает Денис Шуров.

С 1 июня 2017 года система работает в штатном режиме.

РЕЗУЛЬТАТЫ

С момента запуска Deep Discovery Email Inspector позволил отразить 98% атак, в том числе четыре крупные продолжительные таргетированные атаки.

Режим предотвращения атак позволил в разы сократить временные затраты отделов ИБ и ИТ на локализацию и устранение угроз. Email Inspector на данный момент работает практически полностью в автономном режиме.

Освободившиеся ресурсы Банка были направлены на создание специализированной службы по разбору и предотвращению ситуаций, связанных с информационной безопасностью, в том числе и попыток вторжения.

ПЕРСПЕКТИВЫ

В настоящее время в Банке рассматриваются варианты тестирования и внедрения других продуктов компании Trend Micro.

Во II квартале Банк «Санкт Петербург» планирует запустить проект по повышению отказоустойчивости ИТ-инфраструктуры и увеличению мощностей имеющегося оборудования.

Банк заинтересован в продолжении сотрудничества с Trend Micro в том числе и для проведения дополнительных тренингов и семинаров для повышения квалификации своего персонала.

TREND MICRO™

Securing Your Connected World