Cisco SourceFire в «Карлсберг Украина»: надежный щит

Специалисты отдела информационной безопасности ПАО «Карлсберг Украина» и компании ISSP внедрили систему защиты от сетевых атак нового поколения в ЦОД завода в Киеве

Заказчик:
ПАО «Карлсберг Украина»

Отрасль:
Производство пива, алкогольных и безалкогольных напитков

Регион:
Киев, Украина

Интегратор:
Компания ISSP

Решение:

- Проведение комплексного анализа сетевой инфраструктуры пивоваренного завода «Карлсберг Украина» в Киеве
- Определение участков сети с обязательным инспектированием трафика
- Организация «демилитаризованной зоны» и ее защита с помощью системы Cisco SourceFire
- Планируемое обновление межсетевых экранов Cisco ASA для поддержки защиты нового поколения SourceFire
- автоматизация настроек политик безопасности для серверов, рабочих станций и другого оборудования

Преимущества:

- обеспечение надежной защиты для полностью виртуализованного сегмента информационной сети
- интеграция системы SourceFire с процессом управления уязвимостями – сканером Rapid 7
- построение карты сетевых активов и всех служб и приложений с функцией FireSIGHT
- корреляция пользователей из Active Directory с хостами, на которых они работают
- более строгий контроль гостевых соединений

История успеха

Информационная безопасность для производственного предприятия

Три пивоваренных завода компании – в Запорожье, в Киеве и во Львове. Около 1700 штатных и порядка 1300 внештатных сотрудников. Пивные бренды, многие из которых известны без преувеличения во всем мире: «Львівське», «Балтика», «Арсенал», «Славутич», «Славутич ICE», «Жигулевское Запорожского Разлива», «Хмільне», «Квас Тарас», Carlsberg, Tuborg, Zatecky Gus, Holsten, Guinness, Kilkenny, Harp, Warsteiner, Grimbergen, Somersby. Все это – ПАО «Карлсберг Украина», один из безусловных лидеров на украинском рынке пивоварения и один из самых крупных налогоплательщиков страны. По данным отчета аналитической компании Nielsen Holdings N.V. за 2013 год компании принадлежит 27,9% доли рынка пива Украины.

Для успешного, динамично развивающегося производственного предприятия обеспечение безопасности корпоративной сети является одной из самых важных задач. Бизнес-процессы в компании автоматизированы, системы управления ресурсами предприятия (ERP) и системы бизнес-анализа (BI) позволяют решать многие задачи быстрее и эффективнее, но они предполагают активные сетевые взаимодействия, бесперебойные, а главное – хорошо защищенные. Атака на корпоративную информационную систему и компрометация данных могут нанести не меньший вред, чем сбой на производственной линии. Именно поэтому специалистами по информационной безопасности ПАО «Карлсберг Украина» было принято решение внедрить на киевском заводе систему предотвращения вторжений (IDS/IPS).

Учитывая потребности заказчика, в качестве решения мы предложили систему SourceFire. Одним из важных моментов было наличие функционала FireSIGHT, что позволяет в пассивном режиме строить карту сетевых активов и всех использующих их служб и приложений. Кроме того, система позволяет связать активность пользователей с хостами, на которых они работают. После детального рассмотрения предложения заказчик выбрал виртуальные образы под VMware ESX. Это действительно оптимальное решение для режима IDS при мониторинге небольшого сегмента сети.

Сергей Маковец, технический директор
Information Systems Security Partners (ISSP)

Виртуальные сенсоры – реальная защита

Чтобы обеспечить высокий уровень безопасности корпоративной сети, в ходе проекта был создан отдельный сегмент, так называемая «демилитаризованная зона» (DMZ). Задачей системы предотвращения вторжений является анализ входящего трафика из Интернет в DMZ и из DMZ во внутренний сегмент. Таким образом, формируется надежный заслон на внешнем периметре. Необходимая для анализа информация собирается с помощью системы сенсоров, которые внимательно «слушают» трафик.

Главное достоинство системы предотвращения вторжений – ее высокая эффективность. Это касается и эффективности внедрения, и собственно защиты от атак. Внедрение системы SourceFire было делом нескольких дней, а не месяцев, как порой бывает с альтернативными решениями.

После проведения комплексного анализа сетевой инфраструктуры с помощью функции FireSIGHT была создана карта сетевых активов. Кроме того, учетные записи пользователей в каталоге Active Directory были скоррелированы с хостами, на которых они работают. Установка и настройка SourceFire производится действительно быстро, а главное – система хорошо знает сеть и может динамически адаптироваться к любым изменениям.

Не менее эффективным это решение оказалось и с точки зрения эксплуатации, точность срабатывания достигает уровня 99,4% – 99,6%, это очень хороший результат. При этом SourceFire позволяет обнаруживать вирусы фактически «на лету». И в этом данное решение превосходит популярные антивирусы, основанные на сигнатурах. При условии приобретения технологии FireAMP может быть задействован облачный интеллект, который позволяет проанализировать поведение того или иного файла в контексте.

Помимо системы IDS/IPS к анализу трафика, проходящего в защищенный сегмент ЦОД подразделения «Карлсберг Украина» в Киеве, планируется подключить и межсетевые экраны Cisco ASA. Совсем недавно компания Cisco анонсировала запуск сервисов нового поколения FirePower на платформе Cisco ASA. Данное решение добавляет новый сетевой функционал SourceFire к аппаратным платформам Cisco ASA, которые уже установлены у заказчиков. Это позволяет максимально использовать инвестиции в существующие решения безопасности.

Помимо прочих преимуществ SourceFire, для проекта было важно то, что это полностью виртуализированное решение. По сравнению с аппаратными сенсорами, виртуальные, развертываемые под VMware, являются экономически выгодными. Кроме того, такая среда имеет более высокий уровень гибкости: настройки можно менять динамически, «на лету», не внося изменений в аппаратную часть. При этом уровень защиты, разумеется, не ниже, чем у аппаратного решения.

Владимир Илибман,
менеджер по продуктам безопасности Cisco Systems

Результаты проекта

Фактически, результат стал заметен сразу после внедрения системы. Было немедленно выявлено распространение вируса из внешнего сегмента сети. Кроме того, были зафиксированы попытки сканирования внешних ресурсов, в частности VoIP.

Усилился контроль и над гостевыми подключениями, а это важно, так как доступ к информационным системам компании множество внешних партнеров. И используется такая возможность не всегда по назначению: одним из первых результатов работы системы стало обнаружение торрент-трафика из сегмента гостевого WiFi.

ПАО «Карлсберг Украина» удалось создать мощное решение, управляющее сетевыми активами и их уязвимостями. Сенсоры SourceFire обеспечивают надежную защиту выделенного сегмента, в сообщениях о сетевых событиях предлагается детальная информация о происшествиях, включая логин пользователя из Active Directory, имя компьютера и масса других сведений, которые помогают повысить уровень безопасности корпоративной инфраструктуры. Все это обеспечивает перманентную защиту сети. До атаки система позволяет определить надежные политики безопасности в соответствии с нормативными требованиями, во время инцидента она обнаруживает и блокирует атаки, а после него помогает расследовать причину и устранить последствия.

С точки зрения поставленных задач, проект можно назвать успешным. Нам была важна возможность интеграции системы с файерволами Cisco ASA, что обеспечивает автоматизированное и оперативное реагирование на атаки. Коллеги из компании ISSP поделились с нами своим опытом в области сегментации сети и оптимизации ее работы с учетом использования системы IDS/IPS, а также интеграции решения с процессом управления уязвимостями. Тиражирование решения на другие площадки не планируется, так как внешний периметр ограничен ЦОД в г. Киев. Но возможно, мы будем делиться опытом с компаниями Группы Карлсберг.

Александр Бидюк,
специалист отдела информационной безопасности
ПАО «Карлсберг Украина»

Россия, 115054, Москва,
бизнес-центр «Риверсайд Тауэрс»,
Космодамианская наб.,
д. 52, стр. 1, 4 этаж
Телефон: +7 (495) 961 1410,
факс: +7 (495) 961 1469
www.cisco.ru, www.cisco.com

Россия, 197198, Санкт-Петербург,
бизнес-центр «Арена Холл»,
пр. Добролюбова,
д. 16, лит. А, корп. 2
Телефон: +7 (812) 313 6230,
факс: +7 (812) 313 6280
www.cisco.ru, www.cisco.com

Украина, 03038, Киев,
бизнес-центр «Горизонт Парк»,
ул. Николая Гринченко, 4В
Телефон: +38 (044) 391 3600,
факс: +38 (044) 391 3601
www.cisco.ua, www.cisco.com

Беларусь, 220034, Минск,
бизнес-центр «Виктория Плаза»,
ул. Платонова, д. 1Б, 3 п., 2 этаж.
Телефон: +375 (17) 269 1691,
факс: +375 (17) 269 1699
www.cisco.ru, www.cisco.com

Казахстан, 050059, Алматы,
бизнес-центр «Самал Тауэрс»,
ул. О. Жолдасбекова,
97, блок А2, 14 этаж
Телефон: +7 (727) 244 2101,
факс: +7 (727) 244 2102

Азербайджан, AZ1010, Баку,
ул. Низами, 90А, «Лэндмарк»
здание III, 3 этаж
Телефон: +994 (12) 437 4820,
факс: +994 (12) 437 4821

Узбекистан, 100000, Ташкент,
бизнес-центр INCONEL,
ул. Пушкина, 75, офис 605
Телефон: +998 (71) 140 4460,
факс: +998 (71) 140 4465