ИЗДАЕТСЯ КОМПАНИЕЙ «ИНФОСИСТЕМЫ ДЖЕТ»

Jet Info

WWW.JETINFO.RU

ТЕМА НОМЕРА

ПРОЦЕССНЫЙ ПОДХОД К ИБ: ПРИКЛАДНЫЕ МОМЕНТЫ

№ 1-2 (270)/2016

Jet Info

Издается с 1995 года

Редакция:
Дмитриев В.Ю.
Акимова Н.А.
Шедова Е.Л.
Дискина А.Л.

Дизайн и верстка:
Саблина М.А.

Корректура:
Макеева Е.И.

Над номером работали:
П. В. Волчков, А. И. Захаров,
П. А. Кудрин, А. В. Янкин

Издатель:
Компания «Инфосистемы Джет»

Контакты:
тел.: (495) 411-76-01
info@jet.msk.su,
www.jetinfo.ru

АНДРЕЙ ЯНКИН,
руководитель отдела консалтинга
Центра информационной безопасности
компании «Инфосистемы Джет»

О процессном подходе к построению систем обеспечения информационной безопасности сказано уже немало. Сделано, к сожалению, гораздо меньше. Обсуждения процессов обеспечения ИБ и измерения их эффективности редко превращаются в реальные внедрения, вероятно, в первую очередь из-за своей оторванности от практики и реальных потребностей компаний. Вся теория написана для абстрактных корпораций со стремлением к абсолютной безопасности. В результате внедряются средства обеспечения ИБ, которые не обслуживаются, не интегрированы в бизнес-процессы и не дают предсказуемого результата.

Мы решили взглянуть на процессный подход к ИБ с более практической, прикладной точки зрения. В этом номере мы поговорим о том, чего зачастую не хватает нашим подсистемам ИБ, чтобы выдавать ожидаемый от них результат: как заставить работать DLP, как упорядочить хаос управления ролями, как выстроить управление ИБ в рамках SOC и т.д. Следуя установке «не отрываться от земли», мы взяли кейсы из своей практики и на их основе сформировали рекомендации по поддержке ИБ-проектов в части анализа бизнес-задач, построения процессов, обеспечения персоналом и др. Надеемся, что вам понравится.

Содержание

8

18

21

31

3 **От редакции**

5 **Тема номера**
Как комфортно выйти из зоны комфорта
АНДРЕЙ ЯНКИН

8 **Тема номера**
Не забивайте гвозди микроскопом
ПАВЕЛ ВОЛЧКОВ

13 **Собеседник**
Сергей Солдатов,
ЭКСПЕРТ ИБ

18 **Тема номера**
Теория хаоса в отдельно взятой компании
ПАВЕЛ КУДРИН

21 **Тема номера**
Здание SOC: от чертежа до заселения
АНДРЕЙ ЯНКИН

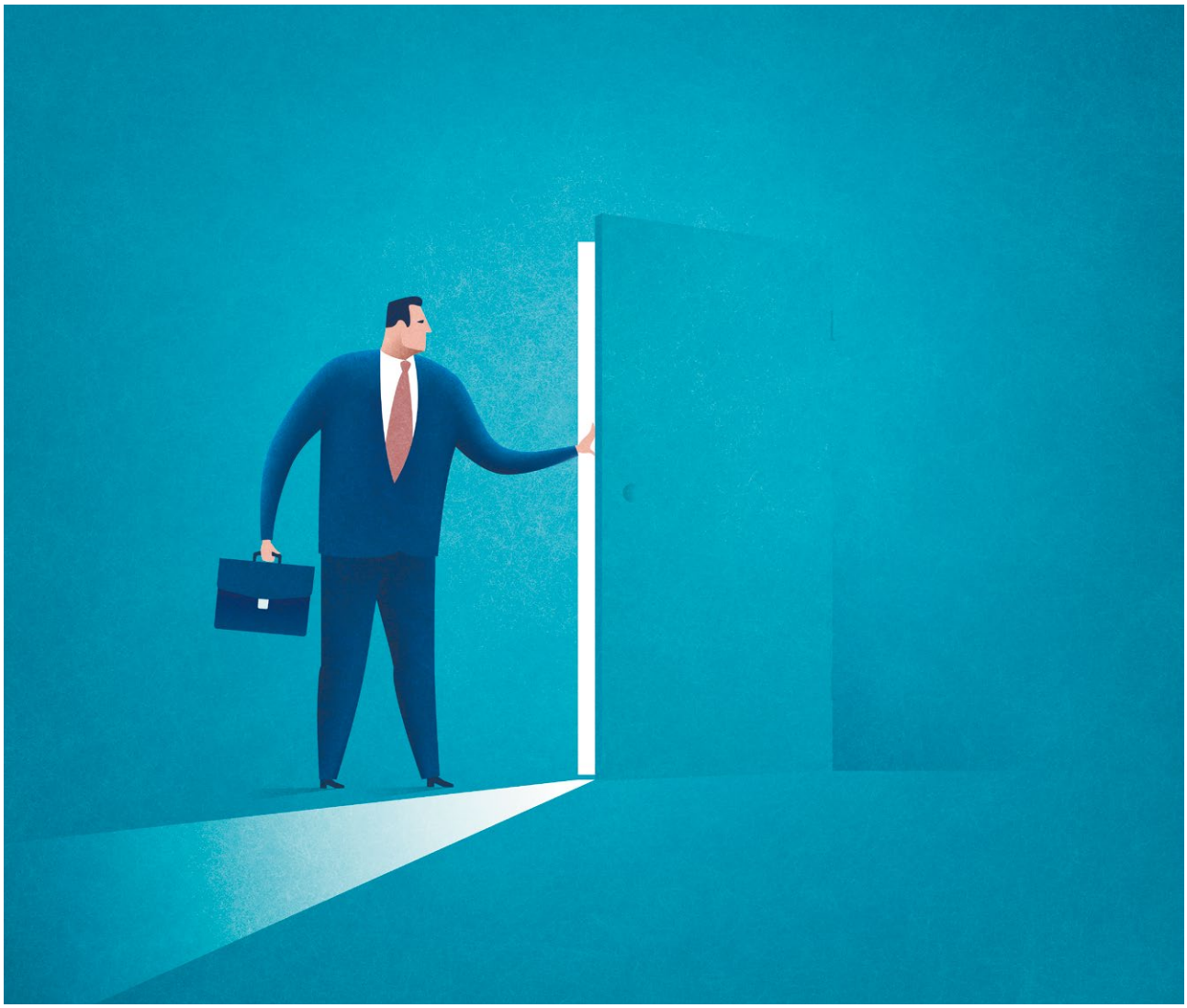
28 **Экспертное мнение**
Быть на одной волне с бизнесом
КОНСТАНТИН СИГАЧЕВ

31 **Тема номера**
Прогулка по граблям, или Почему ИБ не обеспечивает ожидаемого эффекта?
АНДРЕЙ ЯНКИН

35 **Тема номера**
«38 попугаев», или Не все метрики одинаково полезны
АНДРЕЙ ЗАХАРОВ

40 **В тему номера**

КАК КОМФОРТНО ВЫЙТИ ИЗ ЗОНЫ КОМФОРТА



АНДРЕЙ ЯНКИН,
руководитель отдела консалтинга
Центра информационной безопасности
компании «Инфосистемы Джет»

В 2015 году службы ИБ получили серьезную встряску. На фоне сложной экономической ситуации существенно выросли ИБ-риски, при этом бюджеты безопасников зачастую шли под нож. Сокращение штата и урезание вознаграждения порождают нелояльных сотрудников, традиционно являющихся главными нарушителями ИБ. По нашим данным, число инцидентов с кражей конфиденциальной информации, например, случаев воровства клиентской базы, выросло многократно. Сыграла свою роль и активизация конкурентной борьбы, не всегда честной. Редкий интернет-магазин не прощупывали на устойчивость к DDoS.

Служба ИБ должна реагировать на эти вызовы, но ее ресурсы в условиях сокращенных бюджетов довольно ограничены. Приобрести еще одну систему ИБ зачастую нет возможности, с другой стороны, за сытые годы их и так было внедрено немало. Теперь основные усилия брошены на оптимизацию их работы. Перед ИБ-службой встал вопрос о том, как превратить DLP-систему из почтового архива в работающее средство борьбы с утечками информации, а SIEM – из дорогого Log-manager'а в технологическую платформу для оперативного реагирования на инциденты ИБ, как заставить работать IdM.

Медленно, но верно меняется подход и к выбору решений. Рынок продуктов ИБ не только в России, но и в мире в последние годы в значительной степени устоялся. Глобальных переделов рынка или прорывных технологий, сметающих привычное положение вещей, мы не видим. Вполне закономерно, что в каждой нише сформировался определенный паритет. Как правило, есть группа продуктов, которые более-менее одинаково хороши. Или одинаково плохи. В любом случае технологическое преимущество отходит на второй план. Залогом успеха проекта становится не приобретение самого лучшего продукта, а качественная поддержка внедрения и эксплуатации как с организационной, так и с технической точки зрения. Даже решение из второго эшелона при такой поддержке обойдет по эффективности для бизнеса лидера рынка, внедренного формально. Еще и окажется дешевле.

> Безопасность должна помогать бизнесу, быть интегрированной в него. Чтобы строить такую безопасность, нужно, как говорится, выйти из зоны комфорта

Ситуацию с неизменностью рынка отчасти переломил тренд импортозамещения. И здесь качественная поддержка зачастую оказывается важна вдвойне. Не все, но многие российские аналоги пока хромают на одну, а то и на обе ноги. Инженеры строгают костыли, аналитики упорно учат новичка ходить – и о чудо! – аналог начинает довольно резво бегать.

Все эти изменения подстегнули развитие темы, которой мы посвятили ряд статей наших экспертов. Построение ИБ-процессов обсуждается десятки лет, однако до сих пор большей частью остается в плоскости теории. Железо и ПО по-прежнему чаще всего бегут впереди паровоза. Однако в последние годы компании, видя неэффективность технических средств, хотя бы постфактум начинают внедрять процессы ИБ.

Наше участие в этой работе мы называем консалтингом. Однако этот консалтинг – не о стратегиях развития бизнеса в следующие 50 лет. Он носит чисто прикладной характер и решает вполне конкретные задачи:

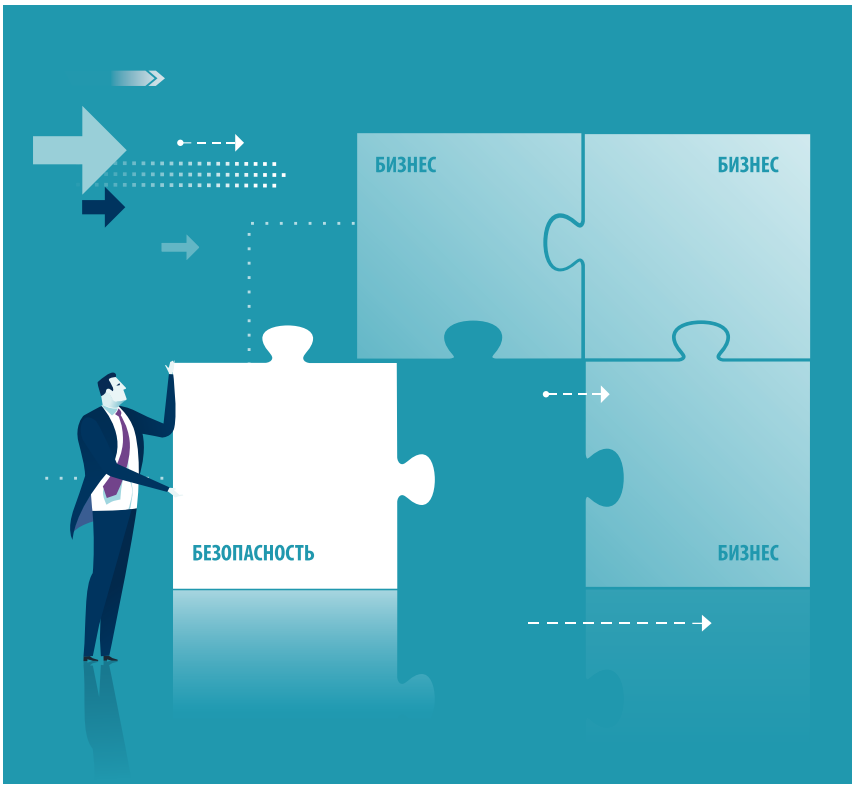
- Как поддерживать в актуальном состоянии систему правил DLP?
- Как с технической и организационной точки зрения выстроить процесс сбора данных инвентаризации со всех дочерних компаний?
- Как подобрать и обучить персонал для дежурной смены SOC?
- Как перейти к ролевой модели управления доступом и какую

часть ИТ-инфраструктуры она должна охватывать?

Подходы к решению такого рода задач мы и обсуждаем. В частности мы решили остановиться на трех темах: на эффективной эксплуатации систем предотвращения утечек информации, построении ролевых моделей и процесса управления доступом и, конечно же, SOC. Это направления, где правильно проведенное обследование и построение процессов ИБ оказывают наибольший положительный эффект на результаты внедрения. Это понимают и наши заказчики. Данные консалтинговые направления стали лидерами роста в нашем Центре информационной безопасности в 2015 году.

Как уже говорилось выше, число инцидентов, связанных с утечкой конфиденциальной информации, за последнее время существенно возросло. Использование DLP-системы для ручного сбора информации и индивидуальное расследование каждого инцидента стали непозволительной роскошью. DLP не на бумаге, а в реальности превращается в бизнес-процесс. Требуются плотное взаимодействие безопасников в части контроля утечек с подразделениями экономической безопасности, правильное использование режима коммерческой тайны, инвентаризация информационных активов и анализ бизнес-рисков. По нашим подсчетам, данное направление показало наибольший рост в этом году из всех консалтинговых проектов Центра информационной безопасности.

Мы давно занимаемся темой управления правами пользователей и построения ролевых моделей, но за последние полтора года таких проектов у нас было больше, чем за предыдущие 6 лет вместе взятые. Отметим, что



существенную часть работы здесь составляет не традиционная ИБ, а анализ бизнес-процессов. Основные причины роста популярности темы, на наш взгляд, – это стремительное увеличение числа и сложности информационных систем в компаниях, необходимость борьбы с внутренним мошенничеством и тенденция к удешевлению IdM-решений.

Отдельно стоит упомянуть о стремительном росте популярности направления Security Operations Center (SOC). В отличие от других ИБ-трендов последних лет, таких как безопасность АСУ ТП, APT или угрозы безопасности интернета вещей, тема SOC меньше подогревалась производителями. Она возникла органично из постепенного совершенствования процессов обеспечения ИБ в компаниях. В одних организациях зрелость процессов ИБ достигла того уровня, когда стала очевидна необходимость объединения их части в SOC для взаимной интеграции и повышения эффективности. Другим компаниям нужен ориентир, к которому можно стремиться при построении ИБ. Среди наших клиентов есть компании, уже построившие SOC в том или ином виде и ищущие пути его дальнейшего развития. Здесь возникает множество сложных вопросов – от построения функциональной архитектуры и выбора KPI до найма персонала и использования аутсорсинга. Все это мы обсуждаем в одной из готовящихся к публикации экспертных статей.

Описываемые подходы выходят за границы чистой ИБ, захватывая не только ИТ, но и основные бизнес-процессы компаний. Безопасность должна помогать бизнесу, быть интегрированной в него. Чтобы строить такую безопасность, нужно, как говорится, выйти из зоны комфорта. Мы говорим о том, как сделать это максимально эффективно и безболезненно. JI

НЕ ЗАБИВАЙТЕ ГВОЗДИ МИКРОСКОПОМ

ПАВЕЛ ВОЛЧКОВ,
старший консультант
по информационной безопасности
Центра информационной безопасности
компании «Инфосистемы Джет»

Представим ситуацию: проснувшись однажды, вы поняли, что ваша DLP работает совсем не так, как вы хотите и давно пора с этим что-то делать. Что именно? Давайте разбираться.

Не будет большим откровением сказать, что эффективность средств защиты информации (СЗИ) прямо пропорциональна зрелости связанных с ними процессов ИБ и их интеграции в бизнес-процесс компании. При этом для некоторых классов СЗИ, например, для антивирусов или средств межсетевого экранирования, эта зависимость выражена не столь сильно. Действительно, в большинстве ситуаций для того, чтобы антивирус работал и обеспечивал защиту на приемлемом уровне, достаточно настроить автообновление сигнатур и следить за состоянием агентов на рабочих станциях, а единожды разработанные списки доступа МСЭ в процессе эксплуатации требуют лишь незначительных изменений. Однако, пожалуй, нет СЗИ, которое бы больше зависело от зрелости сопутствующих процессов ИБ и их интеграции в бизнес, чем система DLP.

Имея опыт реализации более 400 проектов и оказания сервисной поддержки DLP-систем, мы наблюдаем полный жизненный цикл этих решений у ряда компаний (ТЭК, финансовый сектор, ритейл, госсектор и т.д.). К сожалению, некоторые компании находятся в пресловутой ситуации забивания гвоздей микроскопом, когда полнофункциональная система используется эпизодически и/или для решения мелких, локальных задач. При этом в условиях кризисных явлений в экономике, когда обоснование бюджетов на ИБ затруднено, а бизнес требует снижения издержек, поддержка по факту не используемой системы является не самой лучшей идеей, а приобретение средства защиты, которое не будет использоваться, может дискредитировать руководство службы ИБ.

Тем не менее цель нашей статьи – не очередное переливание из пустого в порожнее на тему, почему все так плохо в российской ИБ, а попытка найти решение конкретной задачи: как заставить уже внедренную систему DLP работать эффективнее. Сразу оговоримся, в статье не рассматривается техническая сторона вопроса, лишь организационная.

ОСНОВНЫЕ ПРОБЛЕМЫ

Основной причиной возникновения проблем с DLP являются завышенные ожидания, базирующиеся на не совсем верном с точки зрения «чистого» консалтинга подходе. Этот подход предполагает, что выстраивание процессов вокруг внедренной DLP должно происходить постфактум. Наш опыт говорит об обратном: для эффективного функционирования DLP должна выстраиваться (внедряться) вокруг уже существующих процессов ИБ, а не наоборот. Иными словами, чтобы эффективно использовать DLP, компания должна обладать хотя бы начальным уровнем зрелости ИБ, дорасти до системы.

Приведем главные риски, сопутствующие процессу внедрения DLP:

- **В системе DLP будут реализованы только шаблонные, не отражающие специфику бизнес-процессов правила.**

Согласно принципу сервисного подхода, бизнес-подразделения компании являются «клиентами» службы ИБ, которая оказывает им различные сервисы (услуги), например, защиту от утечек. К сожалению, недостаточное знание своего бизнеса является слабым местом многих ИБ-служб в России. Ситуация с DLP усугубляется тем, что понимание бизнеса должно быть не просто на уровне бизнес-процессов и потоков данных, а еще глубже – на уровне конкретных информационных активов.

> Система DLP может стать отличным помощником в решении огромного количества задач, однако ее настройка и развитие – это не самоцель, DLP – всего лишь инструмент, безусловно, полезный, но не единственный

- **Система DLP «by design» покрывает не все актуальные каналы утечки информации.**

Хрестоматийная ситуация – установка безагентского DLP и одновременное отсутствие контроля съемных носителей. Да, такая DLP позволит выявить сотрудника, который отправил себе на личную почту документы, чтобы поработать дома; да, система может помочь выявить тех, кто бездельничает (чатится, серфит в интернете и т.д.) на рабочем месте, но предотвратит/отследит ли она злонамеренный слив информации? Скорее всего, нет.

- **Реализованные политики будут порождать большое количество ложных срабатываний, которые будет невозможно обработать за разумное время.**

Эта ситуация возникает при первоначальной попытке реализации кастомных правил.

Например, мы хотим отслеживать документы по грифу «Для служебного пользования», а в итоге получаем вал событий, содержащих безобидные фразы «машина для служебного пользования», «прошу выдать мне для служебного пользования» и т.д. Обработать такое количество событий от DLP служба ИБ не в состоянии, и в итоге приходится отказываться от некоторых правил.

- **DLP не предотвращает утечку информации.**

Любая DLP «из коробки» имеет предустановленные словари и правила. Большинство из них направлено вовсе не на защиту от утечек. Найти сотрудников, матерящихся в электронной почте, обсуждающих руководство или рассылающих резюме, может быть интересно и даже полезно, но это, скорее, имеет отношение к вопросам корпоративной этики, а не к защите информации ограниченного доступа.

- **Выстраивание процесса вокруг DLP может негативно сказаться на самом процессе.**

Выстраивание процессов вокруг DLP, а не наоборот, приводит к тому, что организационные меры полностью подстраиваются под доступный функционал внедряемой системы. На практике это сводится к следующей позиции: «Зачем нам регламентировать правила работы со съемными носителями, если мы технически не сможем контролировать выполнение этого регламента».

Итак, что делать, если процессная составляющая отсутствует (по ряду причин: исторически унаследованная система, смена руководства, участие компании в M&A сделках, уход из компании ключевых ИБ-специалистов и т.д.), а DLP уже есть? Решение кроется в методологически верной реализации процессного подхода, учитывающего специфику DLP как средства защиты. Когда речь идет об организации процессного подхода, первое, что приходит на ум, – это классическая модель PDCA (Plan–Do–Check–Act).

В случае с DLP эта модель оказывается наиболее подходящей. Как мы действуем:

- ✓ **Планируем.** Определяем цели системы, какую информацию будем защищать и как.
- ✓ **Делаем.** Реализуем политики DLP.
- ✓ **Проверяем.** Эксплуатируем систему, анализируем получаемые результаты (количество событий и реальных инцидентов, процент ошибок первого и второго рода, результаты тестов, технические показатели).
- ✓ **Корректируем.** Изменяем политики с учетом результатов анализа.
- ✓ **Планируем.** Новый цикл планирования. Учитываем изменившиеся цели, актуализируем информацию, применяем новые подходы.
- ✓ и т.д.

Казалось бы, все достаточно просто, однако свои подводные камни найдутся и здесь.

ПЛАНИРУЕМ

Честное определение цели DLP

Первые сложности могут возникнуть при попытке ответить на простой вопрос «А зачем нам DLP?». При внедрении DLP обычно говорят, что система сможет все и сразу, в то же время в любой компании естественным образом формируется приоритизация задач. Где-то действительно нужно беречь информацию ограниченного доступа, где-то важнее ловить отправляющих резюме, а где-то святая святых – информация о вознаграждениях топ-менеджмента. Определиться, что действительно нужно от DLP, достаточно просто, нужно ответить на ряд вопросов:

> Настройка DLP – многоитерационный процесс, который должен соответствовать известной модели PDCA (Plan-Do-Check-Act). Именно в многоитерационности и постоянном улучшении кроется ключ к реализации действительно функционирующей системы

- Кто основные пользователи DLP, кто планирует пользоваться данными системы (служба ИБ/ЭБ/внутреннего контроля, непосредственно менеджмент и т.д.)?
- Каковы ожидания основных пользователей от применения DLP в ближайшей перспективе (1–3 года)?
- Каковы ожидания руководства компании от использования DLP в перспективе 1–3 лет, хочет ли руководство получать регулярную статистику, и если да, то в каком виде?
- Существуют ли нетиповые внешние требования к компании относительно процесса защиты от утечек информации (например, требования материнских компаний)?

Что конкретно будем защищать

Мы определились с приоритетом – поехали дальше. Следующая потенциальная проблема: как перейти от абстрактных понятий вроде «информация ограничен-

ного доступа» или «информация о топах» к конкретным информационным активам, т. е. как опуститься на уровень конкретных документов, передаваемых между конкретными людьми? Это можно сделать с помощью классического анализа бизнес-процессов, в основе которого лежат инвентаризация и категоризация информационных активов. Это самая важная и сложная задача, которая, по сути, представляет собой отдельный проект по ИБ.

Одна из наиболее созвучных с процессом контроля утечек тем – выстраивание режима коммерческой тайны. Помимо очевидных плюсов, которые режим коммерческой тайны дает сам по себе, он существенно облегчает проведение анализа бизнес-процессов и инвентаризации информации.

Самый главный вклад, который вносит режим применительно к настройке DLP, – преобразование абстрактного понятия «информация ограниченного доступа» в набор вполне конкретных и осязаемых документов. Работая с ними, можно выделять их типовые признаки: формат сообщения, гриф, формат учетного номера, иные особенности оформления, типовые фразы/преамбулы/титульные листы, стандартизированные формы документов и т.д. Другая важная особенность: можно осуществлять более «гранулированный» контроль сотрудников за счет их поименного или подолжностного допуска к коммерческой тайне.

Реальные утечки

Также вне зависимости от того, какое DLP-решение и в какой конфигурации используется, на первом витке планирования целесообразно озаботиться пониманием того, какие каналы утечки наиболее реальны. Сделать это

можно путем проведения небольшого аудита/самооценки по ИБ. По тем каналам утечки, которые не покрываются DLP, необходимо запланировать не менее тщательную работу с использованием других технических и организационных мер. Нужно помнить, что настройка DLP – это не самоцель, DLP – это инструмент контроля каналов утечки, причем один из многих.

ДЕЛАЕМ

Тонкая настройка DLP

Важнейшая составляющая эффективной работы DLP – тонкая настройка политик, а именно создание нестандартных правил в системе. Эта настройка (независимо от применяемого средства и каналов утечки) базируется на трех главных подходах:

- контроль информации ограниченного доступа по ее конкретным выявленным признакам;
- контроль информации ограниченного доступа с помощью признаков типовых документов, одинаковых у всех компаний отрасли;
- контроль информации ограниченного доступа с помощью правил, косвенно позволяющих выявлять инциденты ИБ/аномальное поведение сотрудников.

Как уже было отмечено выше, первый подход – инвентаризация информации и выделение ее типовых признаков – реализуется путем анализа бизнес-процессов и/или деятельности отдельных подразделений. Реализация второго подхода обеспечивается за счет процесса постоянного накопления информации об уникальных правилах DLP и создания баз контентной фильтрации. Целесообразно привлекать к этому вендора или компанию–исполнителя проекта внедрения DLP, т.к. у них уже имеются большие базы контентной фильтрации (типовые акты, формы, шаблоны регулярных отчетов, наборы ключевых слов и т.д.) по отраслям. Отдельно стоит выделить реализацию набора правил, косвенно позволяющих выявить аномальное поведение сотрудников, например, классические отправки шифрованных архивов, пересылка информации на временные почтовые ящики, передача сообщений большого объема и т.д.

Эффективность таких простых, «гигиенических» правил не стоит

недооценивать: они с большей вероятностью помогут обнаружить намеренный слив информации, чем правила, реагирующие на контент.

КОНТРОЛИРУЕМ

DLP – лишь составная часть системы защиты от утечек наряду с процессами и персоналом. Эффективность всей системы в равной степени зависит от каждого ее элемента, при этом создается эффект синергии. В этом смысле интеграция DLP в существующие процессы обеспечения ИБ ценна тем, что позволяет на практике оценить реализованные в DLP политики.

В общем случае DLP связана со следующими ИБ-процессами:

- внутренние коммуникации между службой ИБ и руководством;
- управление рисками ИБ;
- управление доступом к информационным ресурсам;
- регистрация и мониторинг событий ИБ;
- управление инцидентами ИБ;
- повышение осведомленности сотрудников;
- моделирование угроз и нарушителей.

Анализируя эффективность этих процессов, можно сделать вывод об эффективности самой DLP и наметить пути дальнейшей модернизации политик.

Также на этом этапе большое внимание следует уделить борьбе с ложными срабатываниями. Их исключение реализуется путем скрупулезного анализа подробностей детектированных инцидентов и конкретных условий срабатывания для каждого из них.

Другим важным фидбэком, который может быть получен на этом этапе, является демонстрация того, что ранее выделяемых человеческих ресурсов недостаточно для сопровождения системы. Администрирование DLP и разбор возникающих инцидентов являются достаточно ресурсоемкими процессами, особенно если DLP установлено в разрыв. Заранее прогнозировать необходимое количество ИБ-персонала невозможно, все очень индивидуально и напрямую зависит от числа реализованных правил. С нашей точки зрения, необходим, как минимум, один специалист: его главной обязанностью будет сопровождение системы и связанных процессов.

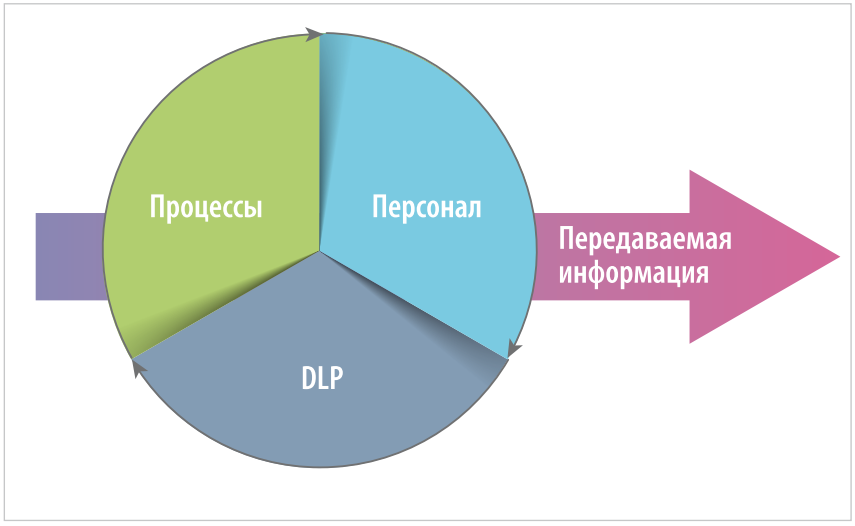


Рис. 1. Составляющие системы защиты от утечек

КОРРЕКТИРУЕМ

Собрав на этапе контроля информацию о фактическом функционировании системы в боевых условиях, необходимо реализовать корректирующие мероприятия, заключающиеся в:

- корректировке имеющихся правил;
- разработке новых правил;
- изменениях ОРД по процессам ИБ;
- выделении дополнительных человеческих ресурсов;
- технической модернизации системы.

Целесообразно включить мероприятия по тюнингу DLP в ежегодный план ИБ-мероприятий.

Отдельно стоит вопрос о том, каким по продолжительности должен быть цикл PDCA. К сожалению, единого рецепта здесь нет, все зависит от сложившихся в компании практик обеспечения ИБ. Мы считаем, что первоначальный этап контроля должен проходить в течение не менее двух кварталов, чтобы гарантированно покрыть собой активности, возникающие в рамках бизнес-процессов компании раз в квартал, например, подготовку квартальной отчетности.

***

Итак, не надо ставить телегу вперед кобылы. Система DLP может стать отличным помощником в решении огромного количества задач, однако ее настройка и развитие – это не самоцель, DLP – всего лишь инструмент, безусловно, полезный, но не единственный.

При этом настройка DLP – многоитерационный процесс, который должен соответствовать известной модели PDCA. Именно в многоитерационности и постоянном улучшении кроется ключ к реализации действительно функционирующей системы. JI

«ЕСЛИ У ВАС ЕСТЬ ЩЕЛКУНЧИК, НУЖНО НАЧИНАТЬ КОЛОТЬ ОРЕХИ»

«Точно так же и с DLP-системой: если она стоит в компании, нужно грамотно, по назначению ее использовать. И одной технической реализации системы здесь недостаточно – нужны выстроенные процессы, постоянная работа ИБ-специалистов по совершенствованию функционирования DLP», – подчеркивает в нашем разговоре о процессной стороне контроля от утечек **эксперт ИБ Сергей Солдатов.**

J.I.: Сергей, наш первый вопрос по факту будет вводным, предваряющим детальное погружение в тему. Что, помимо внедрения технических средств, является необходимыми слагаемыми успеха внедрения системы контроля утечек конфиденциальной информации?

С.С.: Самое главное, что должно быть создано в компании независимо от того, какую систему вы внедряете, – процессы управления ИБ. Нужно проанализировать свои ИБ-процессы, понять, где есть проблемы, наметить и реализовать действия по их устранению. Это первый инструмент корпоративной ИБ-гигиены. Второй – тоже организационный: можно провести классификацию информации, которая используется в компании, выяснить, какие виды информации имеют наибольшие риски с точки зрения утечек и нарушения целостности и доступности, и отработать по ним, для начала оргмерами. Стоит разработать регламенты для сотрудников, описывающие правила обращения с данными, – программу инструктажей. Разобравшись в процессе, определив цели и способы защиты, можно уже подобрать технические инструменты для достижения этих целей.

J.I.: Как нужно проводить обучение сотрудников работе с конфиденциальной информацией, чтобы оно давало максимальный эффект?

С.С.: Имеет смысл проводить инструктаж при приеме сотрудника на работу, а затем

повторно, с заданной периодичностью, например, раз в 1–2 года. Инструктаж может включать в себя рассказ о конкретных кейсах, самых распространенных типах инцидентов, правилах использования информационных ресурсов, которых должен придерживаться сотрудник. Целесообразно проведение тестирования «по горячим следам» – по мотивам полученных сотрудником знаний с установленным проходным баллом. Если человек делает много ошибок, инструктор дает пояснения: почему ответ неверен и как стоило поступить в описанной в тесте ситуации. Завершающим аккордом должно быть подписание новым сотрудником документов, обязывающих его соблюдать установленные в компании правила ИБ.

В обязательном порядке необходимо проводить инструктаж по факту нарушения, чтобы выяснить для себя причины, приведшие к нему, и объяснить пользователю, в чем состоит его нарушение, почему это плохо для компании.

Если у вас есть централизованная база инцидентов ИБ, вы можете вести статистику по подразделениям – кто и что нарушает, какие типы нарушений встречаются чаще. Эта информация должна

> Людям не нужно читать пространные лекции о процедурах ИБ, длинные замысловатые предложения в обучающих документах сразу вызовут негативное отношение. Давайте конкретные кейсы – раз, два, три

фидбэком идти в планы проведения инструктажей и адаптацию программы обучения.

J.I.: Может быть, у вас есть, что называется, проверенные временем рецепты обучения?

С.С.: Очень важно предусмотреть возможность многоканальной обратной связи от сотрудников – это повышает эффективность обучения. Вообще, если человек замотивирован на нарушение, вы его не остановите. Другими словами, если к вам пришел технически подготовленный инсайдер, вы 100%-но не препарируете его своей DLP. Но, к счастью, таких случаев немного. Подавляющее большинство нарушений из моей практики были не преступной халатностью, а просто ошибками, в том числе по незнанию. Вина за подобные ошибки частично лежит и на ИБ-подразделении: незнание – это недоработка того, кто проводит обучение. Может быть, у сотрудника не было возможности спросить, уточнить, как правильно/неправильно, например, какие файлы нельзя отправлять по почте за пределы компании/заливать на публичные файлообменники.

Хорошая тема – короткие, не более трех минут, видеоролики о конкретных случаях нарушений. Истории для видеороликов нужно черпать из практики, по результатам анализа статистики инцидентов. Можно делать скринсейверы на ИБ-тематику, это особенно хорошо работает в open space: человек идет с чаем по офису, а на всех компьютерах в спящем режиме мелькают образы, показывающие как нельзя поступать с информационными ресурсами и носителями информации. Вы получаете перманентное обучение.

J.I.: Как вы относитесь к ограничениям, накладываемым DLP-системой, например, на использование съемных носителей? Эффективны ли они?

С.С.: С ними нельзя перебарщивать. Например, я ограничиваю людям доступ в Интернет, и они начинают пользоваться публичными Wi-Fi-сетями. Мы получаем нулевой результат с точки зрения ИБ и вдобавок недовольных пользователей. Ограничения, как правило, неэффективны, вызывают негатив и мешают людям работать. Правильнее дать сотруд-

никам возможность полноценно использовать корпоративные ресурсы и мониторить их действия, отлавливая нарушения и инциденты, проводя корректирующую работу. Конкретно по обозначенной проблеме: исключите применение съемных носителей для переноса данных между корпоративными компьютерами. Создайте сетевые папки – пусть люди используют их для обмена файлами. Для передачи между компаниями создайте корпоративный файлообменник, доступный партнерам через интернет. Никогда не нужно пренебрегать возможностью контролировать свои данные как можно дольше, а вы контролируете их, пока они находятся на ваших ресурсах.

J.I.: В таком случае какие организационные меры и действия ИБ-специалистов могут являться подспорьем в деле контроля утечек конфиденциальной информации?

С.С.: Навскидку я могу привести пару примеров. Во-первых, помогает реализация принципа круговой поруки, ее модное название – Segregation of Duties. Т.е. нужно исключить ситуации, когда исполнение какой-либо критичной операции закреплено лишь за одним человеком в компании. Сделайте так, чтобы ее подтверждал или контролировал хотя бы еще один сотрудник. Вспоминается старая байка: почему при запуске ракеты нужно одновременно повернуть 2 ключа, находящиеся друг от друга на расстоянии нескольких метров? Чтобы это можно было сделать только вдвоем.

Во-вторых, эффективно использование полиграфов – оно дает хороший процент выявлений. Причем эту функцию можно аутсорсить и регулярно менять партнеров, чтобы в компании не было замотивированного Полиграф Полиграфыча. Использовать этот метод целесообразно в подразделениях, где велик риск мошенничества: закупки, розница.

Но самое главное здесь – повышение лояльности сотрудников и формирование корпоративной культуры, их едва ли можно назвать организационными мерами, но при этом они точно не технические. Здесь наблюдается полное сходство с тем, как патриотизм и любовь к Родине, интегрированные в культуру и воспитание, способствуют снижению вероятности появления недовольных. Вообще корпоративная кадровая и социальная политика – эффективнейший инструмент, позволяющий значительно повысить качество результатов работы сотрудников, однако почему-то об этом мало говорят. Лояльный работник, преданный компании, ценящий корпоративную культуру, будет без дополнительных принуждений делать так, как того требует от него компания: общая корпоративная культура трансформирует исполнение требований в общепринятую практику. В итоге сотрудник не будет напрягаться при исполнении требований, он будет выполнять работу так, как это принято в компании, иначе он не сможет влиться в трудовой коллектив.

> Мой опыт показывает, что сотрудники в подавляющем большинстве лояльны к своей компании. Задача безопасников – поддерживать эту лояльность на должном уровне. Не создавайте своими ограничениями ситуации типа «у меня теперь не печатает принтер/не работает пропуск», дайте людям возможность комфортно работать, тогда они будут стараться соблюдать ИБ-правила. Интегрируйте правила ИБ в корпоративную культуру, и тогда их будет стыдно нарушать

J.I.: Допустим, компания решила использовать DLP-систему «из коробки». Насколько она может быть эффективна?

С.С.: DLP-система – достаточно интимная вещь, ее нужно адаптировать под себя. Чем лучше вы это сделаете, тем больший эффект получите. Я не знаю ни одного успешного кейса с DLP «из коробки», так что не могу сказать, целесообразен ли такой вариант. В то же время я много занимался мониторингом событий ИБ – работал с системами обнаружения вторжений, фильтрации интернет-трафика и считаю, что дефолтные сигнатуры в таких случаях малоэффективны.

J.I.: Если уж мы заговорили о настройке решения, предлагаем обсудить основные принципы, по которым должна жить эффективная DLP-система после внедрения, – без каких регулярных действий она не будет приносить пользу бизнесу?

С.С.: Разумно сначала запуститься в режиме мониторинга, ничего не блокируя, риска в этом нет, поскольку раньше вы жили без DLP вовсе. Должны появиться ИБ-специалисты, которые регулярно анализируют логи системы.

Спустя какое-то время вы поймете, что у вас летает по сети и что из этого создает риски ИБ. Далее обязательно должен быть выстроен процесс обработки результатов работы DLP. Мы выявили инцидент – куда и кому его передавать? Мы можем сообщить о нем специалисту, отвечающему за проведение инструктажей, руководителю сотрудника, совершившего нарушение, и т.д. Во втором случае руководитель, ознакомившись с фактами, принимает решение о дальнейших действиях. Естественно, должно быть не только организационное, но и техническое последствие. Например, мы зафиксировали большое количество drive-by загрузок через интернет-шлюз с последующим сливом чего-то по SSL – имеет смысл запретить загрузку определенного контента с неклассифицированных сайтов. Upload имеет смысл запретить везде, за редким исключением. Например, если с сайта происходит перенаправление на ресурс, который неизвестен нашему категоризатору ресурсов, мы не даем загружать с него PDF, Flash, Java и прочий потенциально опасный контент. Это техническое последствие, по сути, является результатом анализа инцидентов.

J.I.: Что, помимо этого, может проистекать из разбора инцидентов, выявляемых DLP?

С.С.: Процесс регулярного улучшения работы системы. Т.е. мы ставим DLP и начинаем «глазами» смотреть в объем: что летает, кому, куда. Затем анализируем, что из этого – зло, и решаем, как мы будем с ним поступать: блокировать, модифицировать на лету или настраивать другие реакции системы. Например, когда сотрудник увольняется, он обычно начинает сливать данные

на съемные носители. Верно и обратное: если фиксируется большой объем сохраненных на съемные носители данных, например, 500 ГБ за неделю, значит, человек думает уходить из компании. Имеет смысл сообщить об этом факте его руководителю, показать ему список названий файлов, возможно, он узнает среди них документы, содержащие критичную для бизнеса информацию. Далее следует изъятие файлов у нарушителя. И выявление подобных случаев можно поставить на поток: написать скрипт, который в автоматическом режиме будет фиксировать такие факты, установить систему, «автоматом» отправляющую вам письмо о том, что кто-то из сотрудников накопировал себе определенное количество ГБ.

Таким образом, ты используешь свои знания об инцидентах как базу для настройки ИБ-систем под себя. В первый раз ты находишь событие вручную, а затем автоматизируешь поиск подобных случаев. Когда знакомые кейсы у тебя отрабатывает автоматика, ты идешь дальше – находишь новые «болевые точки» и настраиваешь систему под их устранение. Это поступательное движение. Разница между человеком и машиной состоит в том, что человек не работает четко по алгоритмам, он может догадываться, устанавливать и анализировать косвенные признаки. Позднее, когда целостная картина об инциденте собрана, он переводится в разряд стандартных/типовых и автоматизируется, а аналитик приступает к более глубокому анализу, и все повторяется.

J.I.: Какие решения, помимо DLP, целесообразно использовать для контроля утечек?

С.С.: Нужную информацию можно добыть разными путями. Был случай, когда заговор сотрудников одной компании был раскрыт с помощью данных из Skype. Они обсуждали свои планы, используя этот официально разрешенный в компании мессенджер. Дело в том, что клиент Skype кэширует сообщения, ИБ-шники собрали все кэши разговоров и установили, кто именно вел диалог по предмету расследования. Так была найдена вся группа.

Многие системы пишут свои логи, они могут рассказать вам о коммуникациях и действиях сотрудников компании. Причем имеет смысл заложиться в хранилище, чтобы иметь возможность собирать все подряд. А если у вас стоит система их анализа, например, Splunk, логи индексируются и находятся на раз-два.

J.I.: Наш следующий вопрос связан с давним противостоянием между этичностью и практичностью в информационной безопасности. Если гипотетически порассуждать в отрыве от действующего законодательства, нужно ли сообщать сотрудникам о том, что в компании стоит DLP-система и присматривает за их действиями?

С.С.: Афиширование наличия контроля – тонкий момент. Если человек подготовлен и заинтересован в том, чтобы вынести из компании конфиденциальную

Нужно на регулярной основе анализировать причины инцидентов ИБ и исходя из этого формировать план мероприятий по их устранению – как организационных, так и технических. Технические мероприятия должны включать изменения конфигураций ИБ-систем, в том числе DLP.

информацию, он сделает это, что называется, на высоком уровне. Здесь вам поможет только intelligence: нужно очень много всего анализировать и по косвенным признакам вычислять злоумышленника. Если он к тому же будет знать о DLP и принципах ее работы, эта задача еще более усложнится. В любом случае у вас крайне мало шансов его остановить.

Для обычных нарушителей знание о работе DLP не станет панацеей от проблем – часто они случайно совершают ошибки. Другое дело, что сотрудника в таком случае не обязательно сразу вызывать на ковер, можно провести разъяснительные мероприятия, заодно проанализировав его поведение и проверив уровень лояльности к компании. Никогда не нужно пренебрегать возможностью дополнительно побеседовать с человеком. Безопасники любят заострять внимание на железках: если они нормально работают, значит, все хорошо. Но потенциальный ущерб живет не в них, а в бизнес-процессах и в их исполнителях. Так что нужно разбираться в человеческой психологии. Опять же из практики: часто люди поступают неправильно, не потому что они злодеи, а потому что не было возможности поступить правильно – не было нужного сервиса для выполнения их задач, имеющиеся возможности были неудобны или работали плохо, и т.д. Всю эту обратную связь обязательно нужно собирать, чтобы построить удобные и безопасные ИТ-сервисы. Не провоцируйте пользователя рисковать корпоративной информацией из-за отсутствия возможности удобно работать.

J.I.: Каким образом можно измерить эффективность DLP-решения – каковы алгоритмы этой оценки? Имеет ли смысл в принципе измерять эффективность ИБ?

С.С.: Измерять нужно обязательно. Когда ты начинаешь что-то делать, ты ставишь себе цели и задачи. И здесь важно понимать, насколько твои действия приводят к их достижению, делаешь ли ты правильные вещи и делаешь ли ты их правильно. Это и есть мерило твоей эффективности. Допустим, ты борешься с мошенничеством, предотвратил совершение хищений и можешь точно оценить, во сколько бы они обошлись компании. Сравнив это с инвестициями в процесс ИБ, позволивший выявить хищения, можно оценить эффективность. Область незнания – сколько еще невыявленных фактов мошенничества и сколько на этом теряет компания – в расчет при этом брать невозможно, потому что ты не знаешь того, что не знаешь. Нужно опираться на чистые факты: сколько ИБ сохранила компании, столько она стоит.

Важно понимать еще одно назначение метрик: помимо описания того, что было сделано, они позволяют определить слабые места, на которых в будущем следует акцентироваться. На мой взгляд, это наиболее важное свойство метрик, и именно на эту оценку следует бросить усилия, поскольку она позволит адаптироваться к ситуации, совершенствовать свою информационную безопасность.

J.I.: Сергей, большое спасибо за беседу! JI

ТЕОРИЯ ХАОСА В ОТДЕЛЬНО ВЗЯТОЙ КОМПАНИИ

ПАВЕЛ КУДРИН,
руководитель отдела разработки
и внедрения прикладных решений
Центра информационной безопасности
компании «Инфосистемы Джет»

Если компания активно использует информационные системы и у нее большой штат сотрудников, она неизбежно сталкивается с проблемой роста полномочий, которые доступны для запроса пользователям. В некоторых системах количество таких полномочий (ИТ-ролей) исчисляется десятками тысяч, например, в SAP ERP или Oracle ERP количество ИТ-ролей может достигать 250 тысяч. Разобраться в этом списке обычному пользователю очень трудно.

В некоторых компаниях есть специальные отделы аналитиков и методологов, единственная задача которых – принимать заявки на доступ от сотрудников в свободной форме. Затем в информационных системах отбираются необходимые полномочия, и их перечень отправляется на согласование пользователю, который формирует итоговую заявку и повторно отправляет ее на согласование в контролирующие инстанции и на исполнение. Если же такого отдела нет, составление заявки на доступ превращается в длительный и запутанный квест: пользователи начинают самостоятельно искать среди тысяч полномочий необходимые, запрашивать их. После того как заявка согласована и выполнена, выясняется, что часть полномочий не подходит для этого филиала, часть уже не используется, а то, что предоставляется, недостаточно для работы. Кроме того, что на составление заявок уходит время сотрудников компании, на эту же задачу тратит свое время системный администратор, который, вместо того чтобы заниматься администрированием ИС, разбирает поток заявок и назначает десятки полномочий в день. При обследовании в одной из компаний с общим штатом сотрудников в 6000 человек мы выяснили, что администраторы тратили 134 человеко-дня в месяц на разбор и обработку заявок на доступ.

Очень популярны заявки «Мне как у соседа», где вместо соседа вписывается ФИО коллеги, который, как кажется, исполняет схожие должностные обязанности. При этом никто не даст гарантии, что у этого коллеги права не избыточны. Этот ком продолжает расти, и в итоге у сотрудников накапливается огромное количество ненужных полномочий, которые сложно контролируются и могут давать доступ к конфиденциальной информации.

Для решения этих проблем компании часто инициируют проекты внедрения IdM-системы, но без предварительной систематизации доступа. Если она не проводилась в процессе внедрения, результатом становится автоматизированный хаос. Полномочия раздаются и отзываются автоматически, но неразбериха с правами остается.

Оптимальным решением является предварительный проект по оптимизации ролевой модели прав доступа. Самое главное здесь – не увлекаться: часто ответственные за проект стараются распихать 100% всех прав доступа по бизнес-ролям, чтобы при перемещении по должности все роли в ИТ-системах выдавались строго в соответствии с должностью сотрудника и его позицией в оргштатной структуре компании. Этот подход нерационален. Наша практика показывает, что после включения в бизнес-роли ≈80% ИТ-ролей затрачиваемые временные и финансовые ресурсы резко возрастают, и если вовремя не остановиться, на проект можно потратить большое количество ресурсов, но так его и не завершить.

Ролевые модели чаще всего разрабатываются в соответствии со следующими методологиями:

1. **Должностная ролевая модель** – выделение ролей на базе должностных обязанностей сотрудников.
2. **Функциональная ролевая модель** – выделение ролей на базе функциональных задач.
3. **Гибридная модель** – совмещаются подходы должностной и функциональной ролевой модели.

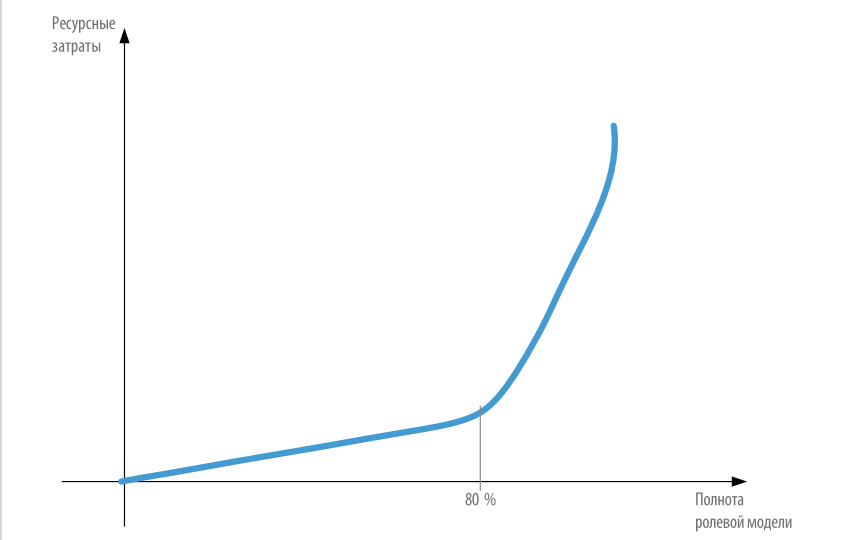


Рис. 1. Зависимость ресурсных затрат от полноты ролевой модели

Роли на базе должностей. Разработка ролей отталкивается от должностных инструкций сотрудников компании. Для каждой должности ответственные за ролевую модель собирают перечень функциональных обязанностей и необходимых полномочий в информационных системах. Этот принцип построения ролевой модели самый очевидный и при этом наиболее сложный как в разработке, так и в дальнейшей поддержке. При этом он наиболее полон в части покрытия ролями потребностей сотрудников.

Основную сложность разработки модели проще пояснить на конкретном примере: если компания большая, в ней может насчитываться около 15 типов бухгалтеров, из них 5 – в одном подразделении. При этом отличия будут только в коде должности. Еще одной сложностью является высокая подвижность оргштатной структуры: в связи с различными бизнес-задачами в течение года она может полностью поменяться, и ролевую модель придется значительно дорабатывать. Несмотря на эти недостатки, подход хорошо подходит компаниям, где жестко соблюдаются регламенты и правила и ведется строгий контроль предоставленного доступа.

Роли на базе функциональных задач. Метод наиболее оптимален с точки зрения соотношения результатов и затраченных усилий. Для построения этого типа ролевой модели в компании выделяют основные и наиболее часто встречающиеся группы ИТ-ролей для запроса, далее они выделяются в отдельные бизнес-роли (например, «доступ в интернет», «годовая отчетность 2016»), которые сотрудник может запрашивать самостоятельно по мере необходимости. Подход в лучшем случае покрывает 70–80% необходимого доступа, оставшиеся роли сотруднику придется набирать из ИТ-ролей.

Гибридная модель. Гибридный подход совмещает 2 предыдущих принципа. Разработка модели для базовых должностей, например, «Кассир», «Бухгалтер», «Инженер», идет следующим образом: выбираются минимальные наборы прав доступа, которые обычно содержат базовые полномочия для этих должностей и назначаются при приеме на работу, а все необходимые сверх этого доступы запрашиваются из функциональной модели или ИТ-ролей. Гибридная модель наиболее востребована на российском рынке, т.к. она гибка в построении и поддержке, умеренна по ресурсным затратам, удобно автоматизируется системами контроля доступа.

Для выделения первоначальной ролевой модели можно использовать специализированное ПО, но, к сожалению, такие решения довольно сложны в установке и настройке. Кроме того, как правило, они очень дороги и не всегда дают нужный результат, т.к. их алгоритмы являются «черным ящиком» и не могут быть оптимизированы под конкретные форматы, использующиеся на российском рынке. Для решения этой проблемы мы реализовали собственный инструмент. В него на вход загружаются данные оргштатной структуры и полномочия сотрудников, а на выходе выдаются 2 вида отчетности: перечень набора ролей для каждой должности из оргструктуры и перечень типовых ролей, которые востребованы у большинства сотрудников компании. На эти отчеты уже намного удобнее накладывать правила разделения полномочий (SoD) и дорабатывать их под требования и регламенты компании.

> Очень популярны заявки «Мне как у соседа», где вместо соседа вписывается ФИО коллеги, который, как кажется, исполняет схожие должностные обязанности. При этом никто не даст гарантии, что у этого коллеги права не избыточны. Этот ком продолжает расти, и в итоге у сотрудников накапливается огромное количество ненужных полномочий

Еще раз отметим, что построение ролевой модели и дальнейшие регламенты по ее поддержанию позволяют не только снизить риски внутреннего мошенничества, упростить процессы управления и контроля назначения прав доступа, но и получить максимальный эффект от внедрения IdM-системы и упростить дальнейшее сопровождение всех ИС компании в части управления доступом. JI

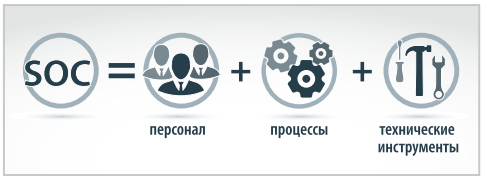
ЗДАНИЕ SOC: ОТ ЧЕРТЕЖА ДО ЗАСЕЛЕНИЯ

АНДРЕЙ ЯНКИН,
руководитель отдела консалтинга
Центра информационной безопасности
компании «Инфосистемы Джет»

Самая большая статья нашего номера не случайно посвящена тематике Security Operation Center. Ведь SOC – это не что иное, как попытка объединения доброй половины процессов обеспечения ИБ под одной крышей для их оптимизации и получения мультипликативного эффекта. И именно здесь мы наблюдаем самые вопиющие попытки подмены комплекса процессов неструктурированной кучей абы как работающих технических средств. Так выгоднее производителям, проще интеграторам, но едва ли такой путь может привести компанию к построению действительно работающего SOC.

Security Operation Center, на наш взгляд, – это не только и не столько технические средства, это прежде всего команда, задача которой обнаруживать, анализировать, реагировать, уведомлять о возникновении и предотвращать инциденты ИБ. Чтобы персонал, вооруженный техническими средствами, понимал свои задачи, имел четкие инструкции и KPI, мог эффективно взаимодействовать внутри SOC и со смежными подразделениями, необходимо выстроить целый ряд процессов в зоне ответственности SOC, направленных на повышение защищенности ИТ-инфраструктуры.

Таким образом, формула работающего SOC выглядит так:



Технические средства важны, но они – лишь инструменты, позволяющие оптимизировать и автоматизировать отдельные процессы в рамках SOC. Неслучайно в сумме это слагаемое стоит третьим.

Конечно же, это не означает, что технические системы вторичны. Без SIEM, IPS, сканеров уязвимости, систем управления заявками, средств анализа дампов памяти и трафика, систем подготовки отчетности и визуализации представить современный SOC невозможно. Мы довольно подробно обсуждали техническую начинку SOC в Jet Info № 8, 2015. В этой статье мы сосредоточимся на вопросах выстраивания процессов и формирования команды SOC.

Рис. 1. Этапы создания SOC

ФОРМУЛИРОВАНИЕ ЦЕЛЕЙ, ЗАДАЧ И КЛЮЧЕВЫХ ПАРАМЕТРОВ SOC

Зачастую при построении SOC первым делом приобретают SIEM-систему. Этот класс ИБ-продуктов прочно ассоциируется с SOC, нередко между SIEM и SOC ставится знак равенства. И только после этого приобретения создатели SOC приступают к конкретной проработке целей и задач системы. Несмотря на туманные результаты такого подхода, он наиболее распространен.

Мы бы рекомендовали немного повременить с SIEM и начать именно с проработки ключевых параметров создаваемой системы: ее функций, архитектуры, задач. Сформулировать это необходимо письменно. Это поможет архитектору SOC самому лучше разобраться в вопросе и донести информацию о миссии и ключевых параметрах системы до коллег, руководства и подрядчиков. Хорошо, если этот программный документ подпишет руководство компании.

На данном этапе имеет смысл задуматься о разработке целевых показателей эффективности создаваемой системы и методов их подсчета.

Изначально лучше сосредоточиться на основных задачах SOC: проактивном предотвращении инцидентов ИБ, обнаружении и анализе нарушений ИБ в режиме реального времени, реагировании на инциденты, а также снабжении всех заинтересованных сторон в компании информацией о текущем уровне ИБ. Остальные задачи можно считать вспомогательными. К ключевым параметрам SOC относятся:

- организационная модель: выделена ли команда SOC в отдельное подразделение или выполнение этих функций распределено между разными специалистами ИБ-службы, насколько SOC централизован, кому подчиняется, каких экспертов может привлекать для работы и т.д.;
- выполняемые функции, проистекающие из задач;
- уровень полномочий: статус специалистов SOC может варьировать от простых «советчиков» (оповещение, предоставление рекомендаций) до «спецназа» (при реагировании на инцидент возможны конфигурирование оборудования, изменение бизнес-процессов, остановка систем и т.д.).

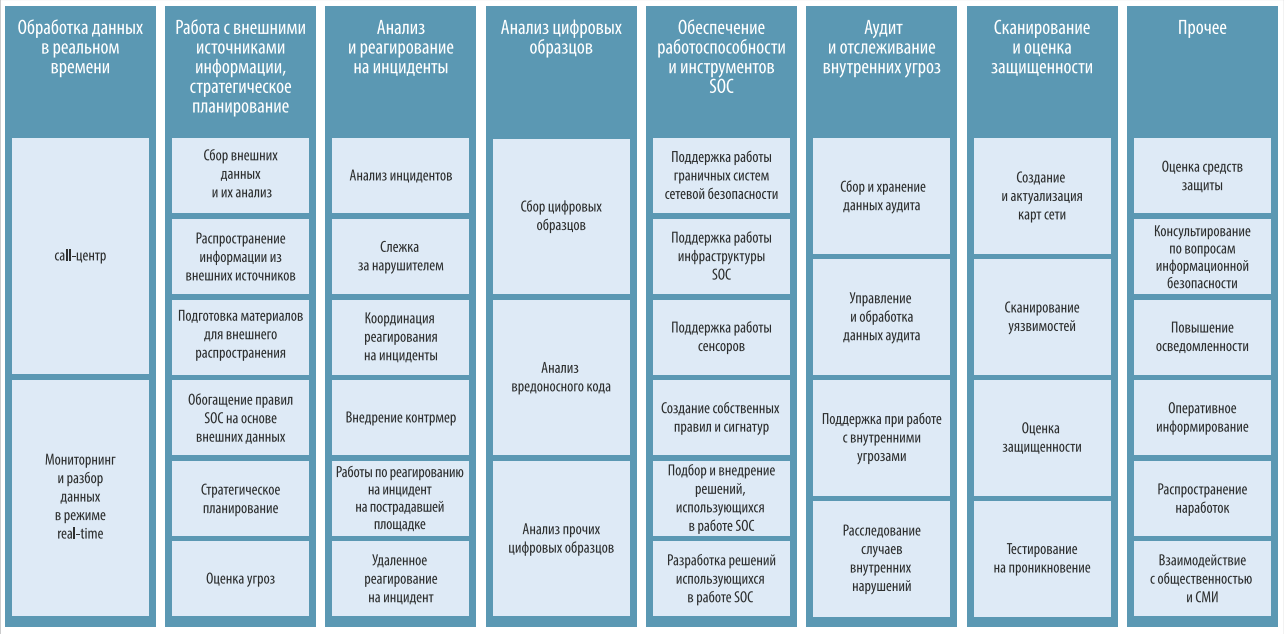


Рис. 2. Основные функции SOC

SOC, обслуживающие внешние компании, обычно рассматриваются отдельно. К таким SOC относятся, например, отраслевой центр внутри группы компаний, SOC, предоставляющий услуги аутсорсинга, и т.п. Вопреки ожиданиям, основные подходы к построению таких SOC те же, что и в случае стандартных корпоративных Security Operation Center.

ОПРЕДЕЛЕНИЕ ОСНОВНЫХ ПРОЦЕССОВ И ПРОЦЕДУР В SOC

Мы выделяем около 40 основных функций, которые может выполнять SOC: от сбора данных об инцидентах до взаимодействия с правоохранительными органами, от анализа вредоносного кода до повышения осведомленности сотрудников о состоянии ИБ (см. рис. 2). Справедливости ради отметим, что мы не встречали в своей практике SOC, успешно выполняющий все эти функции одновременно. Вероятно, таких SOC и вовсе не существует.

Каждый процесс декомпозируется на отдельные подпроцессы и процедуры. Не стоит недооценивать объем этой задачи: за вечер функциональную архитектуру SOC не накидаешь. За 2 дня до написания этих строк мы участвовали в совещании, на котором различные подразделения одной из российских компаний обсуждали процедуру сбора для SOC инвентаризационных данных от дочерних компаний. В итоге возникло такое количество технических, организационных и «политических» спорных моментов, что к концу совещания дискуссия по своему жару не уступала обсуждению годового бюджета. А ведь это, казалось бы, небольшая деталь.

Как было отмечено выше, в начале строительства SOC справедливо правило «меньше, но лучше». Стоит сконцентрироваться на ключевых задачах, стоящих перед создаваемой системой и описать процессы, обеспечивающие их выполнение. Команде SOC нужно иметь актуальную информацию об инфраструктуре, которую она защищает, и эффективно взаимодействовать с коллегами из других подразделений: ИТ-службой, HR, юристами, владельцами систем и др.

Процессы и процедуры лучше фиксировать на бумаге. В компаниях существуют разные уровни документирования, но хотя бы в минимальном виде на этом этапе оно должно быть, чтобы все участники процесса (а их немало) строили одно и то же.

Только теперь, имея представление о том, что именно вам необходимо автоматизировать, можно переходить к выбору технических средств. Помимо традиционной SIEM-системы, вам понадобится множество дополнительных инструментов, зачастую недорогих или бесплатных, но требующих от персонала SOC определенных знаний. Станут вырисовываться и сами требования к качеству и количеству сотрудников.

ПЕРСОНАЛ SOC

Состав персонала, работающего в SOC, определяется выполняемыми им функциями и местом в компании. Здесь возможно огромное разнообразие. Например, сейчас мы принимаем участие в строи-

тельстве SOC в крупном банке и в промышленной компании. В первом случае в SOC также переданы задачи отслеживания фрода, а во втором – мониторинг технической и физической безопасности. Ясно, что для решения таких задач дополнительно нужна команда узких специалистов. Мы же рассмотрим, как обеспечить выполнение основных функций SOC.

Кто нам нужен?

В деле подбора персонала стоит исходить из принципа «качество важнее количества». На ключевых позициях должны быть профессионалы высочайшего уровня. Это тот случай, когда лучше нанять одну «звезду», чем двух рядовых аналитиков (особенно на старте создания SOC).

Поскольку SOC должен оперативно обрабатывать заявки и звонки пользователей, сообщения от различных подразделений компании, информацию из внешних источников и т.д., необходима группа аналитиков.

Для обработки входящей информации мы рекомендуем создать группу первой линии, которая обеспечит выделение в общем потоке в соответствии с принятыми политиками сведений, свидетельствующих об инциденте ИБ. Специалисты первой линии не проводят глубокого анализа сложных инцидентов, их основная задача – оперативно обрабатывать входящую информацию и принимать решения по реагированию на типовые угрозы. Если обработка инцидента занимает больше нескольких минут, инцидент должен быть эскалирован на вторую линию SOC. Эскалации также подлежат инциденты с высоким уровнем критичности. Задержка между получением данных первой линией и эскалацией не должна превышать строго определенного времени (например, 20 минут). В первой линии чаще всего трудятся специалисты среднего и начального уровня (по меркам SOC, разумеется).

> Сейчас мы наблюдаем тенденцию к усложнению внутренних процессов SOC и появлению в них новых измерений: единые центры отслеживают не только инциденты ИБ, но и физическую безопасность, внутреннее и внешнее мошенничество

Сотрудники второй линии должны обладать более глубокими экспертными компетенциями. Они могут расследовать инцидент от нескольких минут до нескольких недель, собирая детальные данные, привлекая экспертов, восстанавливая последовательность действий и готовя рекомендации по ликвидации последствий инцидента, внедрению контрмер и т.д. Посредственные, формально относящиеся к делу сотрудники второй линии сделают неэффективным весь SOC. Здесь нам нужны настоящие эксперты, обязательно обладающие практическим опытом в области обеспечения ИБ.

Рекомендуется осуществлять временную ротацию сотрудников внутри SOC: специалисты второй линии должны часть времени работать в первой, а специалисты первой линии, в свою очередь, привлекаться к расследованию части инцидентов. Эти меры направлены на повышение качества работы SOC, рост профессионального уровня сотрудников и их мотивацию. В течение таких ротаций или в отдельно выделенное время специалисты второй линии (или отдельная команда экспертов) должны совершенствовать метрики, которые используются специалистами первой линии при анализе и эскалации инцидентов, а также анализировать нетипичную и аномальную активность.

Конечно, не каждый SOC может позволить себе 2 линии. Однако такое разделение позволяет наиболее эффективно использовать знания персонала.

Помимо аналитиков первой и второй линии, в SOC чаще всего входят управленцы и администраторы использующихся систем ИБ. Хотя администрирование может осуществляться и другим подразделением или самими специалистами SOC, обладающими, как правило, достаточными для этого компетенциями.

Где искать сотрудников?

Идеальный вариант – найти специалистов, уже имеющих опыт работы в SOC. Однако людей, поработавших в российском, а тем более в западном или азиатском SOC, пока очень мало. Хорошо, если ядро команды составят люди с таким опытом, однако большую часть сотрудников, скорее всего, придется набирать из смежных областей.

Хорошим бэкграундом для сотрудников SOC являются опыт администрирования ИТ-систем и сетевой инфраструктуры (особенно вашей компании), работа в области практической безопасности (в идеале – тестирование на проникновение), опыт программирования. Последнее помогает не только лучше понимать внутреннюю работу систем, но и осуществлять оптимизацию функционирования SOC: писать скрипты, разрабатывать собственные утилиты. Такие небольшие задачи будут возникать

постоянно, и гораздо проще решать их внутренними силами.

Костяк команды должен быть сформирован как можно раньше, чтобы он участвовал во внедрении систем и отладке процессов. Если есть такая возможность, стоит привлечь к работе в SOC часть работающих в компании сотрудников, знающих особенности ее ИТ-инфраструктуры, ИБ-систем и бизнес-процессов.

Сотрудниками первой линии зачастую становятся молодые специалисты с начальным уровнем знаний. Брать вчерашних студентов без опыта работы и обучать их может себе позволить не каждая компания, однако даже небольшого опыта администрирования, как правило, хватает. Разнообразие и интенсивность задач приводят к тому, что специалисты первой линии стремительно набирают опыт. Уже через пару лет многие из них обладают достаточными знаниями и умениями для перевода во вторую линию. К тому же они отлично знают специфику родной ИТ-инфраструктуры. Учитывая тот факт, что хороших аналитиков для второй линии найти сложно, этим источником не стоит пренебрегать.

Обучение сотрудников

Отправить сотрудников на обучение, посвященное техническим средствам, используемым в SOC, – неплохая идея. Оно не сделает из них экспертов, однако позволит быстро сориентироваться в «сложносочиненных» продуктах, таких как SIEM или сканер безопасности. Обучение может провести интегратор или консультанты, участвующие во внедрении системы, причем оно может включать не только технические моменты, но и процедуры, индивидуальные для конкретного SOC. Все новые сотрудники SOC должны обязательно проходить тренинги, знакомящие их с обязанностями, регламентами и техникой. Иначе есть риск однажды обнаружить, что, к примеру, первая линия уже полгода пропускает критичные инциденты. Сбор и распространение внутри команды информации о новых угрозах и трендах в ИБ должны быть не эпизодическими событиями, а отлаженными непрерывными процессами. Важным компонентом обучения является и обмен опытом внутри команды, в том числе при внутренних ротациях.

РЕЖИМ РАБОТЫ SOC

Важный вопрос, который часто вызывает много споров, – режим работы SOC. Ясно, что идеальным вариантом является 24x7 в полную мощность. Многие, особенно направленные атаки, осуществляются ночью. Это приводит к тому, что при работе в режиме 8x5 полноценная реакция последует только к обеду следующего рабочего дня, когда аналитики разгребут завал данных за ночь (или выходные) и разберутся в ситуации.

Однако наш опыт проектов показывает, что расходы на режим 24x7 могут оказаться неподъемными. В сменах работают живые люди, которым необходимы выходные и отпуск. Работа более 8 часов в день в первой линии и 12 во второй не желательна, так как от специалистов требуются внимание и быстрая реакция. Таким образом, только на первую линию нужны минимум 4–5 человек на полную ставку (а ведь желательно, чтобы аналитики еще и страховали и перепроверяли друг друга, а также передавали дела между сменами, получаем все 8 человек). Поэтому зачастую компании формируют промежуточные варианты. Например, 12x5 с двумя пересекающимися сменами по 8 часов в будни и 8 часов в выходные. Аналитики второй линии могут работать при этом в режиме 8x5. На ночь консоль SIEM можно выводить дежурной ИТ-смене, чтобы они отслеживали хотя бы самые критичные ситуации (если для компании это приемлемо с точки зрения безопасности).

Отметим, что найти аналитиков второй линии, готовых работать в ночное время, довольно сложно. С первой линией в этом вопросе, как правило, проще.

Понимая расходы на тот или иной режим работы SOC, а также оценивая актуальные ИБ-риски, компания может выбрать наиболее оптимальную конфигурацию для каждого случая.

ИСПОЛЬЗОВАНИЕ АУТСОРСИНГА

Еще один способ быстрого старта SOC – привлечение сервис-провайдера. Этот подход у нас только набирает популярность, в то время как в Европе и США он уже вполне прижился. Эксперты сервис-провайдера в короткие сроки осуществляют подключение систем компании-клиента к ядру коммерческого SOC и организуют дальнейшее взаимодействие. Оно заключается в информировании компании-клиента о выявленном инциденте, выдаче рекомендаций по его устранению, а также формировании отчета о причинах его появления.

Благодаря использованию этого подхода компания в кратчайшие сроки может выйти на принципиально новый уровень безопасности, однако для этого не достаточно просто подписать договор. Отдать на аутсорсинг все процессы SOC довольно затруднительно, при этом для каждого переданного нужно выстроить часть процесса

на стороне клиента. Чтобы коммерческий SOC приносил пользу, ему необходимы источники данных и их правильная настройка, удаленный доступ к системам компании, всегда свежие данные об инфраструктуре и проводимых работах, понимание специфики бизнес-систем и др. Все это должен обеспечить заказчик.

Сравнение основных параметров своего SOC и аутсорсингового варианта показаны на рис. 3.

Понятно, что аутсорсинг подразумевает определенный набор стандартных сервисов. Построить SOC полностью под себя можно только внутри компании. Немаловажны и вопросы безопасности. Аутсорсинговый SOC обрабатывает крайне чувствительную к разглашению информацию: построение системы защиты, ход расследования инцидентов, учетные записи для удаленного доступа и др. Далеко не каждая компания готова рисковать такими данными. Однако за последние 5 лет заказчики стали относиться к этому несколько проще.

Осознавая все pro et contra аутсорсинга, ряд наших заказчиков выбрал гибридную схему: на первых этапах большая часть задач выносится на аутсорс, параллельно строится свой SOC. Плюсы подхода очевидны. К минусам относится, разумеется, стоимость. К тому же все разработанные правила корреляции и настройки оборудования сервис-провайдер вам наверняка не передаст, особенно бесплатно. Все это, скорее всего, придется делать заново.

Но даже в полностью своем SOC всегда есть место аутсорсингу отдельных процессов, которые держать у себя просто экономически невыгодно. Например, вам раз в полгода нужно провести реверс-инжениринг сложного вредоноса или получить юридическую поддержку в суде. Иметь своих специалистов в таких случаях едва ли стоит.

Параметр	Insource	Outsource
Контроль	Полный	Частичный
Настройка под себя	Полностью	Стандартные сервисы
Скорость развертывания	До 2 лет	Очень быстро
Стоимость	Дешевле через 3–5 лет	Дешевле на старте, OPEX
Качество	???	Предсказуемое

Рис. 3. Сравнение параметров своего SOC и SOC партнера-аутсорсера

ИБ ВНУТРИ SOC

Quis custodiet ipsos custodes?
Лат. «Кто устережёт самих сторожей?»

Важной задачей, которая должна быть учтена при построении архитектуры SOC, является обеспечение безопасности самого центра. SOC должен быть надежной крепостью в море рисков ИБ. Когда падет этот бастион, спасать компанию будет уже некому.

Для SOC нужно разработать отдельные стандарты обеспечения ИБ, строже, чем для всей остальной компании. Инфраструктура SOC должна быть максимально разделена с корпоративной, сетевой сегмент отделен межсетевыми экранами и построен на отдельном сетевом оборудовании. Идея добавить машины SOC в общий домен компании, например, кажется абсурдной, однако мы видим, что это довольно распространенная практика. Стоит исходить из того, что вся ИТ-инфраструктура компании уже скомпрометирована. При построении SOC не стоит забывать, что его глаза и уши – это сетевые сенсоры, IPS, СЗИ, раскиданные по всей компании. Безопасный доступ к ним и их защита должны быть тщательно проработаны. Аналитикам SOC нужен постоянный доступ в интернет и к корпоративным сервисам, и тут рекомендуемое нашей ФСТЭК применение 2 отдельных рабочих станций с KVM-свитчем вполне актуально.

Как и в случае с любой компанией, самые большие риски ИБ для SOC исходят изнутри. Здесь нужно разделять злой умысел и разгильдяйство. Шанс взять на работу потенциального внутреннего злоумышленника не так мал: лучшие ваши аналитики могут иметь практический опыт, лежащий если не в «черной», то в «серой зоне». А хорошее понимание механизмов защиты и детектирования, а также существующих возможностей подзаработать за счет компании делают внутреннего нарушителя очень опасным врагом. Ловить такого инсайдера техническими методами не слишком перспективно. Лучше сосредоточиться на тщательном отборе персонала, внедрить перекрестный контроль работ, ротацию сотрудников и просто не терять бдительности. Что же касается разгильдяйства, выражение «сапожник без сапог»

справедливо в отношении доброй половины ИБ-шников. В любой компании первыми кандидатами на владение 5 лет не обновляющейся ОС являются администраторы ИТ, а вторыми – сами специалисты по ИБ.

Внутренней угрозой может быть и вырвавшийся на свободу зловред, которого аналитик решил проанализировать на основной машине. Для анализа вредоносного кода следует не забыть заложить в проект SOC полностью изолированную «песочницу».

Горячей темой для споров всегда было предоставление информации о работе SOC сотрудникам компании и внешним структурам. Не стоит впадать в одну из крайностей: превращаться в тайную полицию или водить по SOC экскурсии для всех желающих. На наш взгляд, стоит впадать в обе. С одной стороны, SOC должен быть другом и помощником каждого сотрудника компании: сюда можно обратиться при подозрении на инцидент, здесь повышают осведомленность в области ИБ, тут можно получить актуальную информацию о рисках, консультацию, совет. С другой – информация о средствах, методах мониторинга и защиты, ходе расследований должна быть доступна единицам. Причем даже внутри SOC следует проработать ограничения по ее распространению. По поводу обмена информацией с коллегами из других SOC и CERT лучше принять решение сразу: или свести его на нет, или же четко его регламентировать. Никакая конфиденциальная информация не должна попасть к СМИ, в программу конференции или security feed. Второй подход помогает установить полезные дружеские отношения с коллегами и реализовать амбиции лучших аналитиков SOC.

КАК КОНТРОЛИРОВАТЬ РЕЗУЛЬТАТЫ

Качество работы SOC оценить не так-то просто. Подходить к оценке в лоб неэффективно: при повышении качества обнаружения критических инцидентов ИБ становится не меньше, а больше, так как раньше часть из них просто не детектировалась. Аналитики получают новые инструменты, и среднее время расследования сложного инцидента возрастает. Но вместе с тем возрастает и качество.

Однако ввести KPI работы как компонентов, так и целого SOC можно и даже необходимо. Оценка эффективности требуется не только для системы в целом, но и для каждой подсистемы и сотрудника. Иначе ночная смена будет смотреть YouTube, а не пресекать атаки на сетевую инфраструктуру. KPI делают понятной работу SOC для членов команды и руководства компании.

Еще в 1954 году в своей книге «The Practice of Management» Питер Друкер сформулировал критерий SMART, которому должны удовлетворять KPI, чтобы быть эффективными. Показатели должны быть конкретными, понятными, измеримыми, достижимыми, но амбициозными, они должны рассчитываться за строго определенный период или к определенному сроку.

К примеру, параметр типа «хакеры никогда не должны к нам пролезть» – это не KPI. Как это измерить и что это значит? Примерами KPI могут быть, например, «число просроченных критичных инцидентов не более N за месяц» или «суммарное время простоя ключевой системы по вине инцидентов ИБ не более M минут в квартал».

Использованию измеримых показателей эффективности ИБ мы посвятили отдельную статью. Применение KPI позволит быстро выявлять слабые места созданного «штаба компьютерной обороны» и вносить корректировки в его работу.

«ФИЗИКА»

Мы поговорили о процессах и команде, не забыли об ИБ и ИТ-системах, но совершенно обошли стороной еще одну важную составляющую. SOC должен где-то физически располагаться. И оборудование такой площадки – дело нетривиальное. Важно не забыть о физической безопасности, круглосуточном доступе, рабочих местах и информационных панелях, комнате отдыха и др.

Эта тема выходит за границы нашей статьи, хотим лишь дать совет, как к ней подступиться. Ведь данных по этому вопросу немного. На наш взгляд, стоит изучить опыт коллег из смежной области построения ситуационных центров, не связанных с ИБ. Они проработали тему гораздо глубже ИБ-шников и хорошо описали многие подводные камни.

***

Один из наших заказчиков из сферы строительства рассказывал, как принято строить большие здания во Франции: 2 года идут детальное проектирование и планирование работ и затем за 1 год возводится постройка. Этот подход уместен и при строительстве «здания» SOC, если вы не хотите потом по живому прорубать отверстия для забытых труб и копать подвал под построенным домом.

Сейчас мы наблюдаем тенденцию к усложнению внутренних процессов SOC и появлению в них новых «измерений»: единые центры отслеживают не только инциденты ИБ, но и физическую безопасность, внутреннее и внешнее мошенничество.

В таких условиях детальная проработка целей, задач, процессов, макро- и микро-KPI становится залогом успеха построения SOC. JI

КОНСТАНТИН СИГАЧЕВ,
старший специалист отдела информационной безопасности Sberbank CIB

БЫТЬ НА ОДНОЙ ВОЛНЕ С БИЗНЕСОМ

Что ждет бизнес от информационной безопасности? Кто мой заказчик, и каких результатов он ожидает от моей деятельности? В ежедневной рутине стандартных и годами отточенных операций у ИБ-специалиста просто не остается времени, сил и здорового любопытства, чтобы задаваться подобными вопросами. А действительно, сколько раз мы пытались сесть и придумать что-то, как нам казалось, революционное с нуля, преднамеренно нарушая известные еще с университетской скамьи каноны безопасности. Сколько «революционных» методик оценки рисков, проведения аудита ИБ, реагирования на инциденты ИБ приходило в голову каждому уважающему себя эксперту в области информационной безопасности за годы упорного труда? К сожалению, абсолютное большинство даже весьма неплохих идей так и остаются прототипами, которые никогда не будут применены, и у такого положения дел, безусловно, есть негативные последствия.

Нехватка времени, нежелание выходить из собственной зоны комфорта и негативный опыт с «революционными» идеями порождают пренебрежение к деятельности, связанной со стратегическими вопросами безопасности. Кажется, будто бы безопасность вот здесь, близко, в красивых hardening guides от производителей «железа» и софта, в защите периметра от проникновения вредоносного ПО, в обеспечении корректного выполнения процедур контроля доступа к ценной информации, в оперативном реагировании на сообщения из CERT. Список можно продолжать, думаю, каждый узнал в нем элементы своей повседневной работы. И было бы некорректно утверждать, что данные процедуры/процессы/практики (правильное подчеркнуть) не нужны. Так проходят годы, в технологическом развитии ИБ-компонентов наступает стагнация, и, как результат, такая система обеспечения ИБ не способна противостоять современным угрозам.

Таким образом, в проигравших оказывается прежде всего бизнес, ведь для него деятель-

ность любого поддерживающего подразделения – это расход, и, выделяя бюджеты на статьи расходов, связанные с безопасностью, менеджмент справедливо ожидает получить гарантию отсутствия проблем по данному направлению. На деле же проблем меньше не становится: аудиторы по какой-то причине выдают большое количество предписаний, инциденты возникают все чаще, их последствия становятся все серьезнее, пользователи чувствуют неудобство и архаизм манипуляций, которые они должны выполнять для простого получения доступа к файловому ресурсу. Т.е. каждый понимает, что что-то не так с выстроенной системой в целом, но никто не готов проявить инициативу и попробовать поднять вопрос о целях и задачах подразделения ИБ.

Теперь поговорим о таком явлении, как погоня за «революционными» технологиями. Фокус функции ИБ буквально размывается под натиском рекламы и предложений чего-то нового, ранее не известного рынку. Безусловно, ИБ будет всегда находиться в роли догоняющего в свете объема ежедневно возникающих угроз, и такое положение дел заставляет внимательно изучать новинки среди средств защиты. Однако при внимательном взгляде становится ясно, что очередная «новомодная» услуга или средство защиты – это не что иное, как облачение давно изобретенной технологии в красивый интерфейс и привлекательную маркетинговую обертку. Конечно, есть действительно прорывные продукты и услуги, но таких – единицы. Помимо банальной траты денежных средств на первичную закупку и последующую поддержку таких решений, есть еще один серьезный негативный эффект. ИБ-специалисты перестают уделять должное внимание фундаментальным вопросам ИБ: повышению осведомленности персонала, корректной классификации и использованию информационных активов, развитию модели разграничения доступа, разделению полномочий и пр. Мы полагаемся на то, что дорогостоящий продукт разом решит все проблемы, но на деле эффект может быть даже обратным.

> Самое важное и эффективное в деятельности подразделения ИБ – это проактивность. Не стоит ждать грома, чтобы перекреститься. Возьмите за основу общеизвестную мировую методику (например, CIS 20 aka SANS 20 или ISO 27000), составьте список изменений в соответствии с тремя вышеописанными принципами и продавайте их бизнесу

В то же время при общении с коллегами по цеху порой встречается излишняя самоуверенность. Особенно это касается крупных проектов, таких как внедрение систем с большим количеством точек интеграции или создание верхнеуровневой документации по ИБ. Через нежелание объяснять бизнесу необходимость трат на неудобные статьи расходов, например, на консалтинговые услуги в рамках внедрения технологий или процессов обеспечения ИБ, руководители ИБ-служб подвергают риску результат проекта или как минимум получают недостаточный эффект от его реализации. Наиболее часто внедрение системы без оптимизации процессов, которые она должна автоматизировать, заканчивается внедрением «коробки», с которой работает один-единственный специалист, которому это наиболее интересно. Согласитесь, что бизнес, выделяя деньги, ожидал получить совсем другой результат.

Гораздо более эффективным было бы все же отстоять позицию о выделении средств на консалтинг и в рамках проекта разработать набор интерактивных процедур с вовлечением бизнес-пользователей. Таким образом, вы получаете необходимый результат, а бизнес, в свою очередь, его действительно видит, что оправдывает затраченные на проект ресурсы. Бизнес мыслит не «железом» и не программными алгоритмами. Вовлекайте менеджмент в интерактивные процессы – это ему нравится.

Мы придерживаемся трех простых негласных принципов в работе нашего подразделения, и любая организационная и техническая мера обеспечения ИБ должна в той или иной степени им соответствовать:

1. Увеличивай состояние защищенности активов компании.

Самый простой и понятный принцип. Подразделение ИБ должно обеспечивать ИБ. Этот на первый взгляд простой принцип на практике оказывается тяжело выполнимым. Наверное, многие сталкивались с ситуацией, когда

подразделению ИБ исторически делегированы абсолютно не свойственные ему функции. Другой пример: пользователи вынуждены выполнять определенный набор шаблонных операций, которые отнимают у них массу времени, но объяснить их практическую пользу с точки зрения ИБ не могут даже старожилы. Из комментария к этому принципу рождаются следующие два.

2. Снижай нагрузку на бизнес-пользователей.

Безопасники должны решать проблемы не только вселенского масштаба, но и каждого отдельного сотрудника. Старайтесь в своих нововведениях обеспечивать принцип win-win, чтобы, помимо понятного только вам и отдельным стейкхолдерам профита от снижения рисков ИБ, повседневное пользование ИТ-услугами становилось для сотрудников немного удобнее. Например, переход на двухфакторную аутентификацию позволяет снизить сложность запоминаемого пароля, переход на новую версию MDM предоставляет возможность аутентификации через Touch ID, а внедрение IdM позволяет значительно сократить время предоставления доступа к информационным активам для нового сотрудника, чтобы компания максимально быстро начала получать возврат инвестиций в его трудоустройство. Облегчайте жизнь пользователей своими проектами, и вы поразитесь количеству поддержки, которые эти проекты будут получать.

3. Снижай нагрузку на подразделение ИБ.

Помимо банального вопроса эффективности расходования средств на содержание ИБ-специалистов, пагубным фактором, влияющим на продуктивность их работы, является высокий процент нагрузки по операционной деятельности относительно проектной. Поэтому многие руководители ИБ стараются максимально автоматизировать операционную деятельность.

Но самое важное и эффективное в деятельности подразделения ИБ – это проактивность. Не стоит ждать грома, чтобы перекреститься. Возьмите за основу общеизвестную мировую методику (например, CIS 20 aka SANS 20 или ISO 27000), составьте список изменений в соответствии с тремя вышеописанными принципами и продавайте их бизнесу. Подхватывайте инициативы, приходящие от разных подразделений, раскладывайте по структуре перечня запланированных изменений и внедряйте их под эгидой различных, в том числе не связанных с ИБ, проектов. Бизнес ждет от информационной безопасности эффективных действий и результатов – действуйте в рамках тех активностей, до которых можете дотянуться. Современный менеджмент видит в нас уже не специалистов с техническими компетенциями, способных эффективно коммуницировать только посредством CLI, а полноценных бизнес-партнеров, способных не только озвучить проблему на языке бизнеса, но и провести GAP-анализ и предложить на выбор несколько вариантов решения с просчетом показателя cost/benefit. Помимо всего прочего вместе с ужесточением регуляторных требований наши внутренние заказчики как никогда нуждаются в профессиональной экспертизе, так как цена ошибки ИБ-специалиста весьма высока для бизнеса.

В завершение я хотел бы отметить, что внедрение средств защиты не является развитием ИБ, если осуществляется в отрыве от реальных рисков. Наличие современной технологии при отсутствующих базовых процессах обеспечения ИБ дает положительный эффект только в краткосрочной перспективе. Решение о внедрении нового ИБ-средства должно приниматься только когда вы можете ясно ответить на вопрос, какой процесс оно будет автоматизировать, потому что процессы первичны, а задача технологий – оптимизация и снижение ресурсоемкости их поддержки. JI

ПРОГУЛКА ПО ГРАБЛЯМ, ИЛИ ПОЧЕМУ ИБ НЕ ОБЕСПЕЧИВАЕТ ОЖИДАЕМОГО ЭФФЕКТА?

«Внедрили SIEM. Обеспокоенность выросла, безопасность – пока нет».

Кулуарный разговор на ИБ-конференции

СЕРГЕЙ ПАВЛЕНКО,
руководитель отдела инженерной поддержки и сервиса Центра информационной безопасности компании «Инфосистемы Джет»

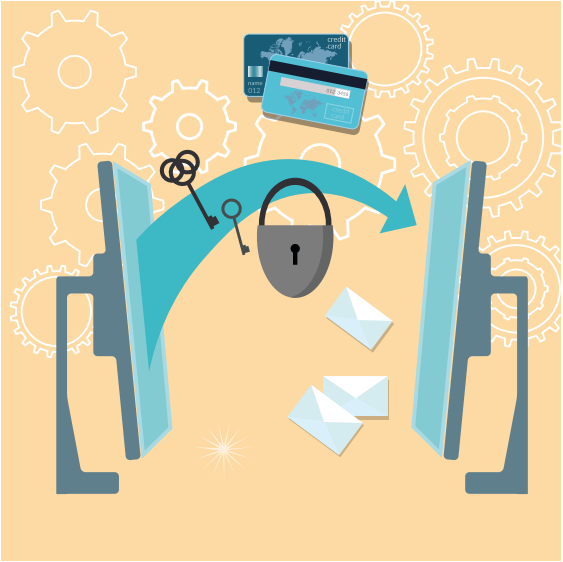
Приходилось ли вам сталкиваться с ситуациями, когда внедренные продукты и решения ИБ не оправдывали ваши ожидания и ожидание бизнеса? Мы постоянно проводим работы на площадках заказчиков и видим, как развивается их ИБ изнутри. На основе нашего опыта мы выделили основные камни преткновения, которые могут приводить к низкой отдаче от внедренных ИБ-решений.

Все очень быстро меняется

Сложность систем ИТ и ИБ сегодня растет очень быстро. Виртуализация, облака, мобильные устройства, удаленный доступ и т.д. – все это значительно усложняет ландшафт угроз и требует построения более сложных систем ИБ. В ответ на новые угрозы вендоры ежегодно предлагают десятки новых решений для защиты бизнеса. И это может порождать хаос в головах безопасников. Во-первых, разобраться в этом множестве новых продуктов по защите информации очень непросто. Только на изучение рассылок вендоров о новых продуктах и актуальных угрозах, посещение тематических вебинаров/семинаров и т.д. у специалиста ИБ может уйти значительная часть рабочего времени. Естественно, немногие могут себе это позволить. Во-вторых, благодаря профессиональной работе маркетинга производителей многие безопасники воспринимают эти новые решения как «волшебные таблетки». Купили, поставили – проблема решена. Разобраться в этом хаосе и выбрать оптимальное решение поможет специализированная ИБ-компания, которая будет выступать в роли независимого консультанта. При выборе такого партнера в первую очередь необходимо обратить внимание на его опыт и репутацию в ИБ-консалтинге.

Недостаточная квалификация ИБ-специалистов в практической безопасности

Наш опыт показывает, что используемые технологии и инструменты обеспечения ИБ могут опережать квалификацию специалистов, работающих с ними. Компании имеют мощные технологии и решения, такие как SIEM, DLP, IPS, NGFW, WAF и т.д., но они не до конца понимают, как применять их с максимальной пользой для безопасности бизнеса. ИБ-отдел ежедневно получает сотни и тысячи событий от различных средств защиты. Что с ними делать дальше?



Для эффективного использования этих решений нужны высококвалифицированные аналитики с разными специализациями: им необходимы глубокое понимание архитектуры Windows и Unix-систем, знания сетевых протоколов и архитектуры веб-приложений, опыт проведения пентестов и анализа защищенности, разработки сигнатур, парсеров и скриптов, опыт анализа Malware. И это далеко не полный список требуемых компетенций. Как найти таких специалистов? Самый быстрый и, наверное, самый дорогой вариант – на рынке. Правда, такие аналитики в дефиците и одним специалистом здесь не обойтись, если, к примеру, у вас есть SIEM, IPS и DLP одновременно. Второй вариант – вырастить специалистов внутри компании. Но на это потребуются годы, и удержать их потом будет сложно. Третий, как нам кажется, оптимальный вариант – воспользоваться услугами компаний-экспертов в области ИБ. В нашей практике есть несколько примеров, когда ком-

Тест на реального безопасника должен включать следующие вопросы:

- ✓ Знаете ли вы, как происходят современные атаки на корпоративные системы? Имеете ли вы представление, как думают и действуют злоумышленники?
- ✓ Имеется ли у вас опыт проведения пентестов?
- ✓ Как вы узнаете, что вас взломали?
- ✓ Имеется ли у вас опыт расследования реальных инцидентов?

пании внедрили у себя SIEM-систему, но так и не научились ею пользоваться. При этом проект по внедрению SIEM – очень дорогое удовольствие. В то же время есть и успешные внедрения (в основном это банки и крупные финансовые организации): компании смогли создать команду «спецназа ИБ», способную адекватно реагировать на возникающие угрозы.

Ситуационный подход к ИБ

Несмотря на то что стандарты управления ИБ существуют уже много лет (возьмем, к примеру, стандарт ГОСТ Р ИСО/МЭК 17799 от 2005 года), в ряде случаев мы видим либо отсутствие у заказчика системы управления ИБ, либо существование ее только на бумаге. Результат такого подхода: латаем дыры по факту их возникновения, существующие проблемы пытаемся решить установкой новых технических средств ИБ, опыт приобретаем путем проб и ошибок, ответственность за инциденты возлагаем на ИБ-отдел. Даже если компания имеет в штате квалифицированных безопасников и внедрила ряд современных технических средств, при отсутствии выстроенных и работающих процессов ИБ все это не будет давать нужного эффекта. IPS работает с политиками и сигнатурами по умолчанию, SIEM используется только как система Log Management, на сервере отсутствует антивирус, в правилах межсетевого экрана permit ip any any – со всем этим мы сталкиваемся в наших проектах. Для того чтобы исправить ситуацию, необязательно иметь сертифицированную систему менеджмента ИБ. Опыт нескольких наших заказчиков доказывает, что пусть и небольшая, но действительно работающая политика управления ИБ позволяет устранить большинство пробелов в системе информационной безопасности.

Не хватает людей

Еще одна из распространенных проблем – нехватка людей в отделе ИБ. С каждым завершенным внедрением на плечи безопасников ложатся дополнительные задачи по эксплуатации новых систем защиты. К примеру, для полноценного администрирования и эксплуатации одной только подсистемы обнаружения вторжений требуется, как минимум, 1–2 выделенных специалиста. В случае же внедрения

По данным PWC, в России в 2015 году по сравнению с 2014 годом:

центра оперативного управления и реагирования на инциденты ИБ (Security Operation Center) необходимо 7–8 человек для обеспечения его бесперебойной круглосуточной работы. Но порой один специалист отвечает сразу за 3–5 подсистем ИБ, например, занимается мониторингом и администрированием SIEM, DLP и DAM одновременно. И не факт, что к этому списку в будущем не добавится еще какая-нибудь система. В одном из банков из ТОП-50 за все подсистемы ИБ отвечают 2 специалиста (SIEM, DLP, Web Gateway, E-mail Gateway, FW, IPS, антивирус, Integrity Control, DAM). Неудивительно, что они могут выделять время только на системное администрирование средств защиты и на устранение сбоев в их работе. Также нехватка людей приводит к низкой вовлеченности специалистов заказчика в процесс внедрения. Из-за этого внедренцам не всегда удается передать необходимые знания о внедряемых решениях, а проект может затягиваться. Но самое важное – от вовлеченности инженеров заказчика в проект зависит качество последующей эксплуатации внедренной системы.

Решить или в принципе не допустить подобную проблему может руководство ИБ-службы компании: нужно понятно и доступно обосновать необходимость выделения новых штатных единиц или передачи части функций ИБ на аутсорсинг.

Формальный подход к ИБ

К сожалению, некоторые компании внедряют системы ИБ исключительно для соответствия требованиям регуляторов. Безопасность при таком подходе выглядит красиво только на бумаге, на деле средства защиты работают с настройками по умолчанию или могут быть даже не задействованы. Из нашего опыта такие компании чаще встречаются в государственном секторе и ТЭК. Говорить об эффективности ИБ в данном случае не приходится.

> Разобраться во множестве новых ИБ-продуктов очень непросто. Только на изучение рассылок вендоров о новых продуктах и актуальных угрозах, посещение семинаров и т.д. у специалиста ИБ может уйти значительная часть рабочего времени. Немногие могут себе это позволить

Неэффективное взаимодействие служб ИБ и ИТ

Службы ИБ и ИТ неразрывно связаны в современной корпоративной системе компании. Эффективность работы каждой службы напрямую зависит от успешности их взаимодействия. При этом наш опыт показывает, что их сотрудничество далеко не всегда выстроено эффективно. Вместо совместной работы по достижению общих бизнес-целей по ряду причин между службами часто возникают конфликты. Приведем примеры. В компании X настройки политик безопасности администрирования межсетевых экранов, прокси-серверов и антиспам-шлюзов выполняет служба ИТ (так сложилось исторически). Фактически ответственность размыта между ИТ и ИБ: формально ИТ-шники не отвечают за систему ИБ, при этом безопасники не имеют необходимых технических компетенций и не могут контролировать выполнение политик безопасности. Отсутствие нужных компетенций негативно сказывается и на авторитете мнения безопасников в глазах ИТ-шников при обсуждении общих технических вопросов.

В компании Y служба ИБ является частью ИТ-департамента и/или подчиняется ему. При разрешении спорных вопросов между специалистами ИБ и ИТ последнее слово остается за ИТ. Вопросы безопасности остаются неучтенными или решаются по остаточному принципу. Например, мы внедряли в компании решение класса Security Gateway Appliance для обеспечения контроля доступа сотрудников к ресурсам Интернет. При обсуждении выбора протокола аутентификации пользователей ИТ-департамент сделал выбор в пользу менее безопасного протокола, не взирая на доводы безопасников.

Специфика взаимодействия подразделений ИТ и ИБ в обоих случаях значительно усложняет процесс внедрения ИБ-систем и негативно влияет на общий уровень информационной безопасности компании.

***

Мы рассмотрели лишь некоторые причины неэффективного использования внедренных ИБ-решений. Отметим, что в условиях кризиса, когда бюджеты контролируются особенно тщательно, компании все больше концентрируют усилия на повышении отдачи от уже существующих ИБ-систем. Способствовать этому может использование процессного подхода, повышение квалификации ИБ-специалистов и использование услуг аутсорсинга ИБ. JI

«38 ПОПУГАЕВ», ИЛИ НЕ ВСЕ МЕТРИКИ ОДИНАКОВО ПОЛЕЗНЫ

АНДРЕЙ ЗАХАРОВ,
эксперт Центра
информационной безопасности
компании «Инфосистемы Джет»

Проблема измерения эффективности мер обеспечения ИБ уже давно стала притчей во языцех. За последние годы на эту тему были опубликованы многочисленные статьи, представлены разнообразные доклады на отраслевых конференциях, организован и проведен не один круглый стол. Но если посмотреть на ситуацию в целом, можно обнаружить, что, несмотря на кажущуюся популярность и востребованность этой темы, в действительности изменилось немногое. По нашим наблюдениям, доля компаний, использующих комплексные метрики для оценки состояния информационной безопасности, за последнее время возросла лишь незначительно. И тому есть объяснение.

Для начала отметим, что практикуемые в компании методы управления ИБ значительно зависят от сложившегося в ней корпоративного управления. Если принятие руководством управленческих решений основывается на качественном внутреннем анализе, то и спрос на Business Intelligence (BI) будет высок. И наоборот, если для оценки ситуации используется ограниченное число высокоуровневых бизнес-показателей, спрос на анализ внутренних процессов будет ограничен. Каждый вариант напрямую влияет на цели и задачи программы измерения состояния ИБ. Главные вопросы, на которые компании необходимо ответить, чтобы эффективно оценивать свою ИБ: для кого создаются метрики и какую информацию они должны нести.

Что по этому поводу советуют эксперты? Для ответа на этот вопрос обратимся к отраслевым стандартам. Пионер стандартизации в области информационной безопасности – NIST – выделяет 4 типа метрик: достижения целей, реализации (выполнения) процесса, результативности (эффективности) выполнения процесса и влияния на бизнес.

Что такое метрики и для чего они нужны? Метрики – это функции, которые используются для измерения чего-либо, например, какого-либо процесса. Можно провести простую аналогию с транспортным средством. Для того чтобы определить, как быстро движется автомобиль, используется метрика «спидометр», какое расстояние было пройдено – «одометр». Обычно формула расчета метрики составляется из тех характеристик процесса, которые представляют наибольший интерес.

Руководящий документ NIST SP 800-55 Rev.1 был разработан почти 10 лет назад, но до сих пор не потерял своей актуальности. В нем хорошо отражена идея индикаторов: результативности (KPI), достижения цели (KGI) и риска (KRI).

Казалось бы, задача понятна, подходы хорошо известны, однако практика показывает, что попытки самостоятельного внедрения системы метрик зачастую

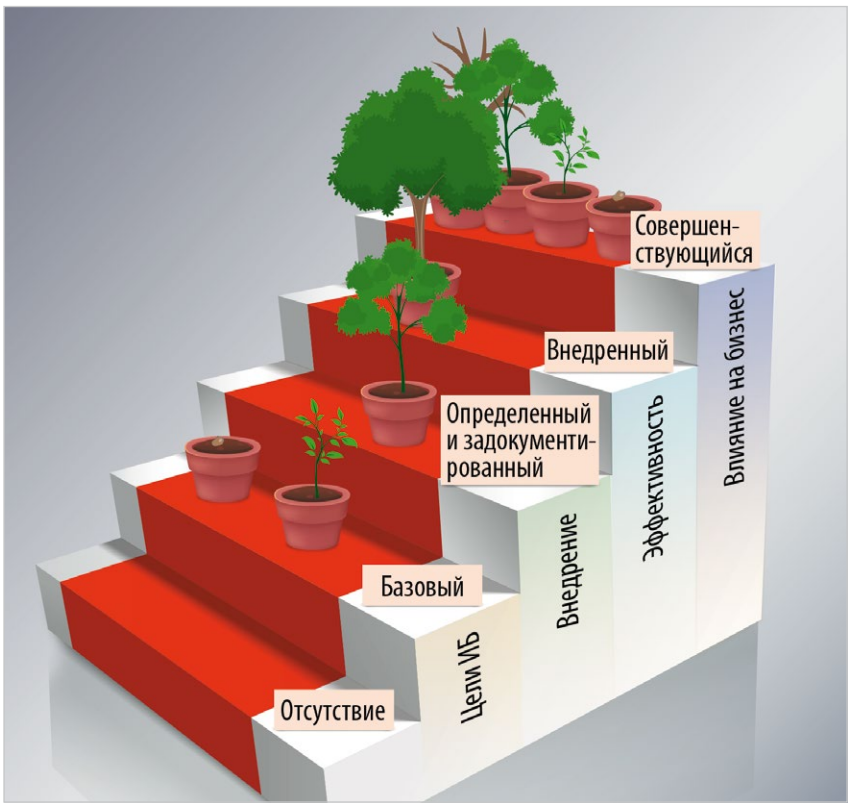


Рис. 1. Уровни зрелости метрик ИБ (по материалам NIST)

заканчиваются неудачей. Это происходит потому, что с самого начала не было соблюдено несколько важных условий. Дело в том, что каждый тип метрик предназначен для определенного уровня зрелости (развития) оцениваемых процессов. Поэтому совершенно бессмысленно конструировать, например, метрики эффективности, если оцениваемые процессы едва удалось документировать.

НАЧАТЬ С САМОГО ПРОСТОГО

Метрики достижения цели позволяют ответить на вопрос о том, были ли решены поставленные ИБ-задачи. Общие цели в области ИБ определены практически в каждой компании. Частные политики и процедуры конкретизируют и детализируют их в разрезе отдельных процессов. Планы мероприятий, в свою очередь, определяют конкретные задачи, подлежащие выполнению.

Метрики достижения цели используются в первую очередь для оценки наличия результатов, поэтому полезны для оперативного управления. Важно отметить, что этот тип метрик ничего не говорит о том, достигается ли желаемый результат на регулярной основе. Для этих целей используется метрика реализации процесса.

СЛЕДУЮЩИЙ ШАГ

Метрики реализации являются следующей ступенькой системы измерения и служат для определения того, в какой мере внедрен конкретный процесс. Они используются в том случае, когда деятельность уже формализована в виде процесса, но он еще не внедрен полностью. К примеру, управление уязвимостями требует наличия процесса их выявления. В том случае, если он выполняется только для 70 систем из 100, можно говорить о 70%-ной его реализации.

Этот тип метрики является относительным и требует наличия установленных пороговых значений, с которыми будет сравниваться измеренный результат. Определение пороговых значений – отдельная задача, порой еще более сложная, чем основная, поскольку 100%-ный результат любой ценой далеко не всегда является целесообразным. Отметим, что метрики реализации в основном предназначены для руководства ИБ-подразделения, поскольку позволяют отслеживать прогресс внедрения процессов обеспечения ИБ.

ВХОДИМ ВО ВКУС

Метрики результативности выполнения процесса, стоящие еще на одну ступеньку выше в иерархии метрик, сфокусированы на конкретных показателях деятельности и отвечают на вопрос, насколько результативно работает тот или иной процесс или защитная мера, будучи внедренными. К примеру, одна из целей процесса повышения осведомленности пользователей в области ИБ состоит в минимизации числа инцидентов, связанных с использованием методов социальной инженерии. Если в результате обучения пользователей в 8 случаях из 10 они не поддаются на провокационные письма и звонки злоумышленников, можно сказать, что показатель результативности процесса (для этой цели) составляет 80%. Данный тип метрик также является относительным и требует определения пороговых значений, с которыми будет сравниваться результат.

Для того чтобы учесть фактор стоимости ресурсов, которые затрачиваются для достижения желаемого результата, используются метрики эффективности. Зачастую они являются производными от метрик результатив-

✓

Крупный российский оператор связи разработал и внедрил систему метрик информационной безопасности в поддержку недавно утвержденной стратегии в сфере обеспечения ИБ. Разработанные метрики охватывали не только уже существующие процессы обеспечения ИБ, но и те, которые еще предстояло внедрить. Для удобства подготовки отчетности для руководства, курирующего блок информационной безопасности, расчет метрик был автоматизирован. Почти сразу же возникла проблема, связанная с некорректностью расчета метрик, поскольку они описывали состояние пока еще не реализованных процессов обеспечения ИБ. Так как руководство интересовали обобщенные показатели состояния ИБ, общая картина получилась смазанной в худшую сторону, несмотря на то что текущее состояние ИБ было достаточно высоким.

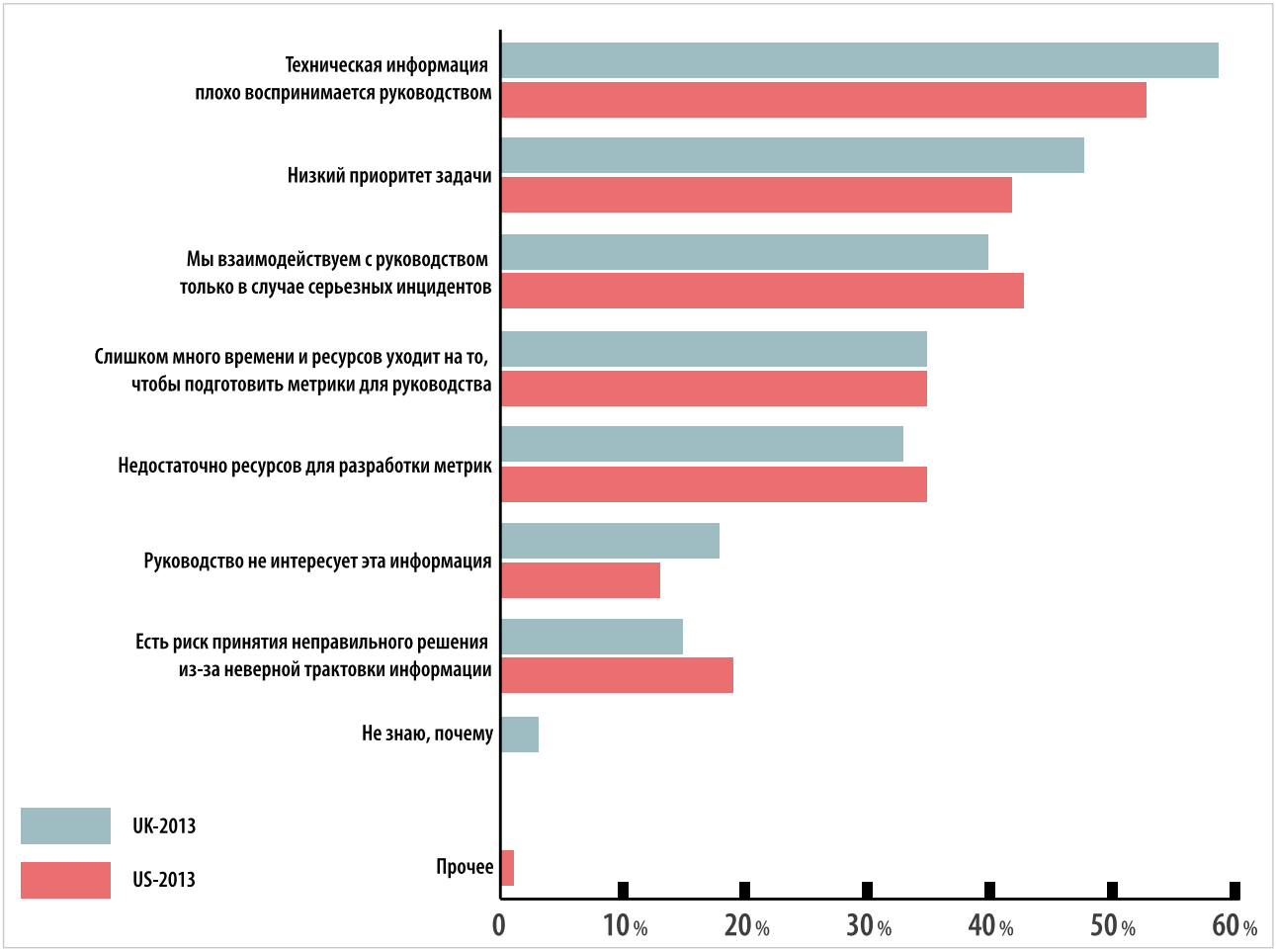


Рис. 2. Основные причины отсутствия бизнес-ориентированных метрик ИБ в западных компаниях (по данным Ponemon Institute)

ности. Метрики эффективности могут высчитываться по формуле «результативность/стоимость», где в качестве стоимости могут выступать любые используемые ресурсы: деньги, персонал, время, или их комбинация. Если потребителями метрик результативности являются руководители подразделения ИБ, то метрики эффективности могут быть интересны руководству компании, курирующему ИБ-направление.

ПОСТИЧЬ ДЗЕН

Наконец, последний тип метрик – метрики влияния на бизнес. Он является самым сложным с точки зрения наполнения. Эти метрики отвечают на вопрос, в какой степени результаты конкретных мер обеспечения ИБ влияют на показатели бизнес-деятельности.

Бизнес в конечном счете всегда интересуют доходы, соотнесенные с рисками, поэтому первое, что приходит в голову в качестве критерия измерения, – это риск-ориентированные метрики, поскольку это общая цель для всех процессов обеспечения ИБ. Отношение показателя результативности (эффективности) конкретной меры ИБ к величине ожидаемых потерь (ALE) по защищаемому активу или процессу – неплохая бизнес-метрика, отражающая меру адекватности защитной меры существующему риску. Однако зачастую возникает проблема, связанная с недостаточно развитым процессом анализа рисков в компании. Поэтому этот подход не универсален.

Другой путь – выбрать несколько бизнес-целей, очевидным образом зависящих от успехов (или неудач) в области ИБ, и создать метрики на их основе. В результате масштабного исследования, проведенного Ponemon Institute в 2013 году, выяснилось, что более половины организаций вообще не применяют бизнес-ориентированных метрик ИБ, поскольку не в состоянии оценить фактическое влияние ИБ на бизнес.

Для решения этой сложной задачи можно воспользоваться

концепцией системы сбалансированных показателей (Balanced Scorecards, BSC). На рис. 3 приведен пример бизнес-ориентированных метрик ИБ, вписанных в систему ценностных перспектив BSC.

РАЗМИНКА ДЛЯ УМА

Рассмотрим использование системы метрик измерения эффективности ИБ на простом примере. Предположим, мы задались целью приобрести автомобиль. Попробуем сконструировать набор метрик, который поможет нам измерить успех этого мероприятия на всех его этапах.

Прежде чем стать обладателем автомобиля, нам необходимо выбрать желаемую комплектацию, сравнить цены в автосалонах, решить вопрос с финансированием покупки и, собственно, приобрести машину. Метрика достижения цели будет определяться степенью выполнения всех перечисленных задач в процентном отношении. Дополнительно можно учесть вес/важность каждой задачи.

Метрик реализации может быть несколько – по одной на задачу (иногда больше). К примеру, если мы решим задействовать средства на покупку из нескольких источников, можно использовать метрику, которая будет характеризовать объем уже собранных средств в сравнении с целевой суммой. Аналогично можно оценить число автосалонов, которые мы посетили, по сравнению с планируемым.

Предположим, мы успешно справились со всеми задачами, но пока этим занимались, самые интересные комплектации во всех автосалонах раскупили, и нам пришлось купить автомобиль с более скромными характеристиками. Метрика результативности нашей покупки характеризует то, в какой степени наш автомобиль соответствует тому, что мы хотели получить, чего мы ожидали. Можно привести множество метрик результативности: оценку разгонной динамики в сравнении с эталоном (например, заявленным изготовителем), шумоизоляцию, экономичность и т.д.

Метрика эффективности покупки в данной ситуации будет определять, насколько привлекательную цену мы заплатили за эту комплектацию, не переплатили ли или не слишком ли залезли в долги.

Наконец, эквивалентом бизнес-метрик будут являться метрики влияния совершенной покупки на нашу жизнь. Насколько продуктивнее мы стали использовать свое время, передвигаясь на автомобиле? Как изменились наши расходы в связи с приобретением? Какие новые возможности у нас появились благодаря наличию автомобиля? Список можно продолжать.

Рис. 3. Пример бизнес-ориентированных метрик ИБ

В КАЧЕСТВЕ ЗАКЛЮЧЕНИЯ

Отметим, что ключ к получению действительно эффективных метрик – их регулярное тестирование как на этапе конструирования, так и при последующем использовании. Данные, на основании которых должна рассчитываться метрика, могут попросту отсутствовать, быть некорректными или неактуальными. В этой ситуации метрика будет приносить больше вреда, чем пользы. Необходимо всегда отталкиваться от имеющегося фактологического материала, учитывать цели и задачи создаваемых метрик и по возможности автоматизировать весь процесс. JI

МНОГОКРАТНО ВОЗРОСЛА ВАЖНОСТЬ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ВЕБ-СЕРВИСОВ

Введение санкций, импортозамещение, девальвация рубля, спад в экономике – все эти факторы сформировали новую ситуацию на рынке ИБ, которая привела к перераспределению структуры и спроса, и предложения. **Директор Центра информационной безопасности компании «Инфосистемы Джет» Алексей Гришин** рассказывает CNews о том, как меняется расклад на рынке, объясняет, каким образом происходит оценка эффективности внедрения ИБ, что меняется в специфике борьбы с мошенничеством и киберпреступлениями и пр.

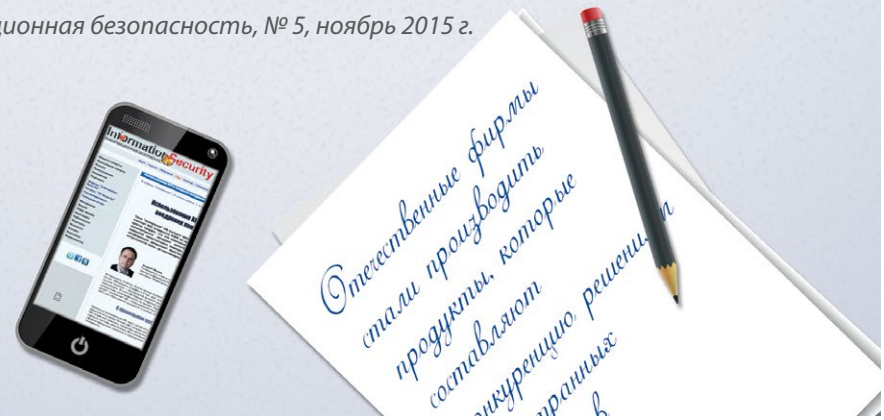
Источник: CNews.ru, декабрь 2015 г.

ИСПОЛЬЗОВАНИЕ KPI В ПРОЦЕССЕ ВНЕДРЕНИЯ КОНТРОЛЕЙ ИБ

АВТОР: АНДРЕЙ ЯНКИН

Тема «измерения» ИБ сегодня чрезвычайно популярна. И это понятно: бизнес всегда пытался измерить ИБ «общим аршином». В итоге ИБ-бюджет существенно уступает бюджету ИТ, а сотрудников катастрофически не хватает. **Андрей Янкин, руководитель отдела консалтинга Центра информационной безопасности компании «Инфосистемы Джет»**, описывает способы переломить сложившуюся ситуацию и роль понятных количественных KPI в этом процессе.

Источник: Информационная безопасность, № 5, ноябрь 2015 г.



ТЕХНОSOC: МОНИТОРИНГ СОСТОЯНИЯ ИБ ТЕХНОЛОГИЧЕСКОГО СЕГМЕНТА ПРЕДПРИЯТИЙ

АВТОР: ДАНИИЛ ТАМЕЕВ

Построение SOC сегодня практически любой организацией воспринимается как необходимость. Причем в банковской сфере и оборонно-промышленном комплексе ситуация перешла на уровень выше – этим вопросом озаботились и соответствующие регуляторы. Однако, по мнению **Даниила Тамеева, руководителя направления по работе с ПиТЭК Центра информационной безопасности компании «Инфосистемы Джет»**, при запуске проектов по построению SOC в предприятиях промышленного сектора и ТЭК часто упускают из виду важность расширения зоны его действия и на технологический сегмент. Подробнее о том, что такое техно-SOC и в чем его особенности – в статье Даниила.

Источник: Connect, № 10, октябрь 2015 г.

РЕЦЕПТЫ SOC: ГОТОВИТЬ САМИМ, ПРИГЛАШАТЬ ПОВАРА ИЛИ ЗАКАЗЫВАТЬ ПО МЕНЮ?

АВТОР: ТИМУР НИЯЗОВ

При достижении определенного уровня зрелости ИБ, любая организация сталкивается с задачей управления инцидентами ИБ. И в первую очередь в этом случае решается вопрос о способе реализации: строить собственный SOC самостоятельно, отдать его построение на откуп интегратору или использовать аутсорсинговые сервисы. **Тимур Ниязов, менеджер по продвижению SOC и защиты баз данных Центра информационной безопасности компании «Инфосистемы Джет»**, в своей статье рассматривает нюансы всех вариантов и признает, что каждый имеет право на существование (в зависимости от конкретной ситуации).

Источник: BIS Journal / Информационная безопасность банков, № 4, октябрь 2015 г.

ЧТО ЗАКАЗЧИКИ ОЖИДАЮТ ОТ DLP-СИСТЕМ?

АВТОР: МИХАИЛ АНОШИН

О том, что ожидают заказчики от DLP-систем, на что необходимо обратить внимание при выборе решения и что еще, кроме DLP, можно использовать для повышения эффективности управления доступом к информационным ресурсам, на экспертном круглом столе рассказывает **Михаил Аношин, руководитель направления DLP Центра информационной безопасности компании «Инфосистемы Джет».**

Источник: «Информационная безопасность», №3, июль 2015 г.

КРИЗИС DLP-ТЕХНОЛОГИЙ: А БЫЛ ЛИ МАЛЬЧИК?

АВТОР: МИХАИЛ АНОШИН

С технологической точки зрения DLP-продукты достигли (или в ближайшее время достигнут) потолка в своем развитии – все возможные «фишки» в части способов контроля информации средствами DLP уже придуманы, и с 2011 г. никаких технологических прорывов в этой сфере по большому счету нет. Можно ли считать это кризисом? Каковы его последствия и надо ли их минимизировать? На эти и другие вопросы в своей статье отвечает **Михаил Аношин, руководитель направления DLP Центра информационной безопасности компании «Инфосистемы Джет».**

Источник: «Информационная безопасность», №3, июнь 2015 г.

Jet Info infosystems

Jet Info
ИЗДАЕТСЯ КОМПАНИЕЙ «ИНФОСИСТЕМЫ ДЖЕТ»

Главный редактор Дмитриев В. Ю.

Россия, 127015, Москва, Б. Новодмитровская, 14/1,
тел. (495) 411 76 01, факс (495) 411 76 02, e-mail: Jetinfo@jet.msk.su, www.jetinfo.ru

Полное или частичное воспроизведение материалов, содержащихся в настоящем издании, допускается только по согласованию с издателем