В последние пару лет о SOC (ситуационном центре информационной безопасности) не говорил только ленивый. Многие крупные организации либо уже имеют SOC в каком-то виде, либо задумываются о его создании. В чем же сложности обеспечения эффективной работы SOC, когда все необходимые технические средства у компании уже есть и ответственный персонал назначен? Какие основные векторы атак должен выявлять любой SOC?

Топ-9 уязвимостей: как справиться с ними при помощи SOC?

Андрей ГАЙКО,
Digital Compliance, заместитель генерального директора

Основные функции SOC — это мониторинг защищенности инфраструктуры, управление инцидентами ИБ, контроль соответствия требованиям (комплаенс) (рис. 1). В каждом из этих направлений SOC должен решать определенные задачи:

1. Мониторинг защищенности инфраструктуры включает в себя поиск и устранение уязвимостей, анализ внешних и внутренних источников об актуальных киберугрозах и выработку защитных мер, сбор, анализ и аудит журналов событий с IT-/ИБ-систем.

2. Управление инцидентами предполагает выявление, анализ, реагирование на инциденты и выработку мер по совершенствованию действующих процессов/средств ИБ на основании полученного опыта.

3. Контроль соответствия требованиям включает технический контроль за выполнением требований стандартов ИБ и регуляторов в IT-/ИБ-системах.

Статья основана на нашем опыте проведения аудитов в финансовых организациях как в области комплаенса, так и в области анализа защищенности. Такая практика позволяет с обеих сторон посмотреть на SOC (или на то, что под этим термином подразумевают).

В первом случае, при оценке соответствия процессов ИБ требованиям регуляторов, мы можем увидеть, как работают процессы ИБ, реализующие задачи SOC: в частности, работа с уязвимостями, создание новых правил в SIEM, реагирование первой и второй линий

Андрей ГАЙКО

Рисунок 1

Основные функции SOC

на инциденты. Нам предоставляется возможность оценить, как в действительности происходит реакция на инциденты, и сделать выводы, насколько существующие порядки и планы реагирования адекватны и эффективны.

Во втором случае, если проверяемая компания публично не заявляла о том, что у нее есть SOC или сотрудники компании нам об этом не сообщали, то пентестеры не смогут однозначно понять, следит за ними кто-то или нет. Со стороны атакующего SOC не виден. Как говорилось ранее, одной из функций SOC является мониторинг защищенности инфраструктуры. Теоретически SOC должен выявлять злонамеренные действия пентестеров и реагировать на них. Поэтому с другой стороны баррикад нам становится понятно, есть ли реакция на наши действия или нет.

Имея объективный взгляд с двух сторон баррикад, попробуем понять, в чем же сложность в обеспечении эффективной работы SOC, когда все необходимые технические средства у компании уже

Топ-9 уязвимостей: как справиться с ними при помощи SOC?

есть и ответственный персонал назначен. После этого рассмотрим несколько основных векторов атак, которые должен выявлять любой SOC и нужным образом на них реагировать. «Настройка» SOC на выявление и блокирование этих векторов атак позволит пресекать более 80% реальных инцидентов информационной безопасности.

Какие проблемы сопутствуют «настройке» SOC?

Несмотря на то что с каждым годом средства защиты совершенствуются, усложняются и автоматизируют все больше «человеческих» функций, слабым звеном всегда является человек. Типичны случаи, когда в компании существует недопонимание или даже открытая вражда между IT- и ИБ-отделами. У каждого из подразделений есть свое видение зон ответственности другого. Подразделение ИБ может считать, что ему не нужно вникать в используемые в инфраструктуре технологии и достаточно дать IT-отделу высокоуровневые требования по безопасной настройке систем. IT-отдел в свою очередь не сомневается, что отдел ИБ должен выдавать конкретные требования по настройке конкретных систем. На выходе получаем, что время идет, а системы не сконфигурированы или сконфигурированы недостаточно безопасно. Учитывая возрастающее количество используемых технологий и вводимых в эксплуатацию систем, получаем большое количество «белых пятен» в информационной инфраструктуре.

Еще одним негативным результатом в связи со сложностями в отношениях отделов IT и ИБ является упущение из вида отдела ИБ новых систем, появляющихся в IT-инфраструктуре. Зачастую количество запросов от бизнеса к IT на новые изменения, разработку и развертывание новых систем превышает разумное количество. Это ведет к тому, что отдел IT вынужден постоянно создавать новые серверы, устанавливать новое ПО. При большом количестве таких задач вопросы безопасности отодвигаются на второй план, ведь главное — это потребности бизнеса и скорость ввода в эксплуатацию. Поэтому возникают ситуации, когда технические задания забывают согласовать с отделом ИБ либо делают это нарочно для ускорения процесса или запрос на изменение проходит мимо отдела ИБ. Не важно, какая была причина, важно, что в итоге отдел ИБ не был уведомлен об изменениях. Из-за этого пропадает контроль за безопасностью новых систем и возникают потенциальные риски информационной безопасности.

Для более эффективной «настройки» SOC самым правильным, но трудоемким является подход, при котором специалисты по ИБ следят за постоянно меняющимся IT-ландшафтом, имеют знания и, главное, понимание того, какие возможности предоставляют исполь-

Андрей ГАЙКО

зуемые в компании системы. Это позволяет определить потенциальные слабые места в используемых технологиях и дает возможность формулировать более конкретные требования к безопасной настройке систем. В свою очередь, зная технические особенности систем, можно более корректно создавать правила обработки событий в SIEM, делать более тонкие настройки аудита на конечных узлах. Это снизит количество «белого шума», создаваемого SIEM, и позволит следить только за действительно важными событиями. Несомненно, такой подход потребует от специалистов по ИБ технических навыков и постоянного повышения своей компетенции, но для эффективной работы SOC другого пути нет.

В отдельную категорию проблем стоит выделить психологические особенности людей. Поясним на примере. У одной компании в плане реагирования на инциденты для первой линии SOC — службы мониторинга событий ИБ — было указано, что для определенных зарегистрированных событий необходимо звонить сотруднику, который был инициатором такого события, и узнавать у него, почему он выполнил такие действия. Когда такое событие наступало, но нарушителем был не рядовой сотрудник, а один из руководителей подразделений, ответственный за звонок не делал звонка, так как стеснялся побеспокоить начальство. Случай банальный, но показательный. Люди могут чего-то не делать из-за своих личных качеств. Реагирование на инциденты подразумевает общение с сотрудниками на разных уровнях корпоративной иерархии, и к этому всем нужно быть готовыми.

Для более эффективной «настройки» SOC самым правильным, но трудоемким является подход, при котором специалисты по ИБ следят за постоянно меняющимся IT-ландшафтом, имеют знания и, главное, понимание того, какие возможности предоставляют используемые в компании системы.

При разработке планов/инструкций реагирования на инциденты следует учитывать «человеческие» особенности как сотрудников SOC, так и остального персонала.

Несомненным плюсом является поддержка деятельности отдела ИБ высшим руководством. Если руководство заинтересовано в информационной безопасности компании и демонстрирует это, то и с деятельностью отдела ИБ начинают считаться остальные отделы. Это дает сотрудникам отдела ИБ больше уверенности в себе и в своих действиях, делает их работу более важной в глазах окружающих.

Топ-9 самых популярных уязвимостей

Поскольку наиболее важная деятельность SOC — это выявление и реагирование на инциденты информационной безопасности, стоит более подробно описать наиболее часто применяемые векторы атак. Несмотря на кажущуюся банальность описываемых векторов, они действительно работают. Тут можно провести аналогию с веб-уязвимостями. Все разработчики и все специалисты по безопасности

Топ-9 уязвимостей: как справиться с ними при помощи SOC?

знают, что такое SQL-инъекции, как их выявлять и как с ними бороться. При этом данный вид уязвимостей остается наиболее популярным и действенным при внешних атаках. Возникает вопрос: если всем прекрасно все известно, то почему статистика не меняется?

Типичный злоумышленник не пользуется сложными технологиями для компрометации систем. Поиск уязвимостей нулевого дня и создание работоспособного ПО для их эксплуатации — процесс длительный и сложный. Подобное программное обеспечение стоит достаточно больших денег. Поэтому с большой долей вероятности злоумышленники будут использовать наиболее простые и не менее эффективные средства для достижения поставленных целей.

1. Слабые пароли

Документированные парольные политики есть практически во всех организациях. Часто во время комплаенс-аудита приходится общаться с сотрудниками на местах и спрашивать их о действующих в компании политиках безопасности: читали ли они эти документы, что из них помнят, как применяют их на практике. Нередко сотрудники не могут назвать требования к паролям. К числу таких сотрудников относятся и сотрудники IT-подразделений, которые непосредственно заняты конфигурированием систем. Это приводит к тому, что при вводе новых систем парольные политики не конфигурируются, учетные записи по умолчанию не изменяются.

Схожие результаты мы получаем на практике при тестировании на проникновение. Пентестеры для начала проводят простую проверку: сканирование сети, обнаружение сервисов/систем с попыткой аутентификации с использованием общеизвестных учетных записей и паролей, установленных производителем данных сервисов/систем по умолчанию. Очень часто это срабатывает, и мы получаем доступ к ресурсам.

Решение этой проблемы в рамках SOC лежит на поверхности. Прежде всего нужно организовать более качественное повышение осведомленности сотрудников о требованиях к учетным записям и паролям. На техническом уровне — сделать правила мониторинга, отслеживающие вход в системы с использованием учетных записей, созданных производителем по умолчанию, либо периодически выполнять сканирование подсетей на наличие возможности входа под учетными записями, установленными производителями по умолчанию.

2. Man-in-the-middle

Существует множество техник перехвата данных в сети. Наиболее популярными и действенными являются arp-спуфинг и NetBIOS-

Андрей ГАЙКО

спуфинг. Большинство современного сетевого оборудования имеет встроенные методы защиты от атак данного типа. Однако администраторы пренебрегают этими настройками, и такие атаки удачно проводятся. Если с обнаружением и защитой от arp-спуфинга все более или менее понятно, то NetBIOS-спуфинг достаточно сложно детектировать. Стоит отметить, что в нашей практике еще не доводилось встречаться у клиентов с детекторами NetBIOS-спуфинга.

Чтобы обеспечить детектирование спуфинговых атак, следует определить, в каких подсетях они возможны, настроить IDS/IPS и сетевое оборудование на обнаружение и (или) блокировку этих атак, а также включить оповещение. Что касается устаревшего протокола NetBIOS, то от него стоит отказаться в принципе и отключить его поддержку на всех хостах.

3. NTLM

NTLM-протокол широко применяется в Windows-сетях. Администраторы боятся полностью отказаться от этого протокола из-за возможных проблем с устаревшим ПО.

Существует пул атак, эксплуатирующих особенности этого протокола. Из наиболее популярных можно назвать smb-relay, pass-the-hash. Именно они самые часто используемые и эффективные.

Для защиты от атак на NTLM-протокол следует полностью перейти на Kerberos-аутентификацию и отключить поддержку NTLM, хотя многим специалистам это покажется слишком радикальным решением. Одним из новых методов обнаружения атак с использованием извлеченных хэшей паролей является HoneyTokens/HoneyHashes. Методика подразумевает загрузку в память машин с ОС Windows заведомо известных хэшей паролей для определенных учетных записей. В SIEM следует сделать правила для выявления всех фактов использования таких учетных данных. Поскольку злоумышленник не может знать, что за учетные данные он смог получить, он начнет пытаться осуществить вход в системы с их применением. Любое использование этих учетных данных в информационной инфраструктуре однозначно даст понять, что действует злоумышленник.

4. Привилегированные и системные учетные записи

На четырех из пяти инструментальных аудитов успешно реализуются атаки, связанные с запуском прикладного ПО под учетными записями приложений, имеющих системные права. Типичным является случай, когда на сервере устанавливается веб-сервер и он запускается как сервис с системными привилегиями. Далее возможны

варианты. Либо на сервере забывают отключить функциональность, позволяющую входить на веб-сервер без авторизации и устанавливать свои приложения, либо на веб-сервере запускается уязвимое приложение, взлом которого позволяет выполнять чужой код. В обоих случаях все сводится к загрузке на исполнение программного кода злоумышленника с системными правами на целевой машине. Это дает полный контроль над сервером, после чего он используется как отправная точка для дальнейшей атаки. В 60% случаев именно уязвимость этого типа приводит к получению злоумышленником прав уровня доменного администратора.

Для предотвращения подобных инцидентов необходимо наделять учетные записи приложений и сервисов ограниченным набором прав в объеме, необходимом им для корректного функционирования. В SIEM следует создать правила, отслеживающие создание учетных записей приложений, изменения прав доступа для таких учетных записей. В качестве организационной меры нужно документировать порядок ввода и настройки новых систем и донести эту информацию до всех системных администраторов.

5. Обновление ПО

В 2014 г. весь мир узнал о таких уязвимостях, как Heartbleed и Shellshock. Под ударом оказались миллионы систем. Несмотря на то что истории были громкими, а с тех пор прошло два года, вплоть до сегодняшнего дня мы часто сталкиваемся с наличием Heartbleed в клиентских системах.

Обычной практикой в компаниях является использование устаревшего ПО. У таких систем часто закончен срок их поддержки производителем и выпуск обновлений безопасности прекращен либо обновления выходят, но обновление систем технически сложно сделать. Эксплуатируя уязвимость Heartbleed, становится возможным вытащить из оперативной памяти устройства имена учетных записей и пароли к ним в открытом виде. Ни разу наши специалисты не видели, чтобы имеющиеся у клиента IDS/IPS как-то реагировали на эксплуатацию этой уязвимости, притом что во многих сканерах безопасности (как платных, так и бесплатных) существуют сигнатуры, позволяющие с легкостью определять, устойчива ли система к этой уязвимости.

Поскольку одной из функций SOC является анализ уязвимостей в информационной инфраструктуре, необходимо сканировать на наличие указанных уязвимостей все возможные устройства и системы, не забывая о legacy-системах. В IDS/IPS следует включить проверку трафика на соответствующие сигнатуры.

Андрей ГАЙКО

6. Системы/интерфейсы управления оборудованием

Существует целый класс систем удаленного управления и мониторинга аппаратной части серверов. У разных производителей они называются по-разному, но суть одна. Имея доступ к консоли управления подобной системы, становится возможным выполнять любые действия с сервером.

Как правило, системы управления и мониторинга серверами выделяют в отдельный сетевой сегмент для ограничения к ним доступа. Но, как показывает практика, доступ из других, в том числе пользовательских, подсетей к этому сегменту остается. Это связано с тем, что при наличии большой информационной инфраструктуры администраторы опасаются по максимуму ограничивать сетевой доступ в такие сегменты из-за возможных проблем с работоспособностью данных систем, сложностью своевременного восстановления вышедших из строя или нарушивших свою работу серверов. В итоге к системам управления предоставляется избыточный доступ.

В 2013 г. исследователями безопасности был выпущен отчет с описанием потенциальных уязвимостей в данных системах, после чего в публичном доступе появились соответствующие эксплойты.

Поскольку в компаниях к системам предъявляются достаточно серьезные требования касательно бесперебойности их работы, а для обновления систем управления необходимо останавливать работу серверов, то системы своевременно не обновляются или не обновляются вовсе. Выходит, что довольно устаревшие эксплойты могут сработать. В связке с избыточным доступом вероятность взлома систем управления многократно возрастает.

Для своевременного обнаружения факта применения эксплойтов против систем управления и мониторинга серверами следует включить на IDS/IPS соответствующие сигнатуры и следить за сообщениями об атаках. Хорошим вариантом будет развертывание honeypots в инфраструктуре с заведомо устаревшими системами управления.

7. Новые веб-технологии

Почти все современные приложения — это веб-приложения. Причем вектор развития веб-технологий движется в сторону усложнения веб-систем. Если раньше веб-приложения писались самостоятельно от начала и до конца, то теперь разработчики используют множество сторонних фреймворков, протоколов и API. Как следствие, у систем появляется множество верхнеуровневых взаимодействий — фреймворки на различных платформах общаются между собой. Возникают различного рода коллизии, которые могут эксплуатироваться зло-

Топ-9 уязвимостей: как справиться с ними при помощи SOC?

умышленниками для компрометации систем или доступа к критичным данным. Кроме того, никто не отменял веб-уязвимости. Из года в год разработчики утверждают, что они знакомы с техниками безопасного программирования, у них большой опыт написания кода и они следят за безопасностью. И из года в год наиболее популярными уязвимостями остаются SQL-инъекции, xss, csrf и прочие из списка OWASP top-10.

Нельзя отрицать серьезность последствий компрометации внешних и внутренних веб-систем. SOC необходимо отслеживать веб-запросы и на основании полученного опыта проводить тонкую настройку межсетевого экрана прикладного уровня.

8. Фишинг

Большую эффективность имеют фишинговые атаки на сотрудников компаний. Это подтверждает как наш собственный опыт, так и общемировая статистика. Из множества вариаций фишинга выделяется несколько наиболее популярных. В первом случае на e-mail сотрудников рассылаются письма, содержащие в качестве вложения вредоносное программное обеспечение. Во втором случае в письме содержится ссылка на веб-страницу. На первый взгляд такие ссылки визуально похожи на доменные адреса атакуемой компании. Дизайн фишинговых веб-страниц неотличим от дизайна веб-страниц иных ресурсов компании. Такие страницы имитируют формы ввода учетных данных для входа в корпоративную систему.

Одной из задач SOC является противодействие фишингу. Существует достаточно действенный способ защиты от перехода сотрудника по ссылке в фишинговом письме. Необходимо взять название корпоративного домена второго уровня и с помощью специальных генераторов сгенерировать все возможные вариации названий этого домена. Также рекомендуем дополнить этот «словарь» названиями, которые вы сможете придумать самостоятельно. Например, если у вас домен называется company.ru, то следует перебрать все возможные варианты написания, визуально схожие с оригиналом: c0mpany.ru, cmpany.ru, compny.ru, sompany.ru, copany.ru и т.п. Далее нужно настроить перенаправление запросов внутренних корпоративных пользователей к этим ресурсам на ваш внутренний ресурс путем настройки корпоративного DNS. Тем самым сотрудник при нажатии на ссылку попадет не на фишинговый сайт, а на контролируемый вами ресурс. Это самый дешевый и простой способ. Что касается вредоносных вложений, то тут все сложнее. Самые известные вредоносы смогут быть замечены антивирусным ПО. Если стоит

Достаточно действенный способ защиты от перехода сотрудника по ссылке в фишинговом письме: взять название корпоративного домена второго уровня и с помощью специальных генераторов сгенерировать все возможные вариации названий этого домена, далее настроить перенаправление запросов внутренних пользователей к этим ресурсам на ваш внутренний ресурс путем настройки корпоративного DNS.

Андрей ГАЙКО

задача защититься от таргетированных фишинговых атак, то поможет лишь поведенческий анализ.

9. Антивирусы

Что бы ни говорили производители антивирусного ПО, обнаружение вредоносов в 99% случаев выполняется на основании сигнатурного анализа. Основной функцией антивирусного ПО можно назвать предотвращение эпидемий известных вирусов. Превентивные функции защиты не спасают от неизвестных вендору вредоносов. В арсенале вирусописателей имеется большая гамма способов обхода антивирусов. В рамках тестов на проникновение специалистами используются «болванки» зловредного ПО, которые не обнаруживаются антивирусами. Поэтому при защите информационных ресурсов не стоит сильно полагаться на антивирусное ПО. Как уже было сказано, если злоумышленник решил использовать непубличное вредоносное ПО, то на помощь придет только поведенческий анализ.

На основании описанного вырисовывается вполне ясная картина вариантов векторов атак и шагов злоумышленников (рис. 2).

В заключение приведем пару кейсов по выявлению кибератак.

Пример 1

На один крупный банк с общей численностью сотрудников более 2000 человек была проведена атака. Сотрудники получили персональные письма с вложением. Более пары сотен человек открыли это вложение. Служба информационной безопасности своевременно выявила факт заражения компьютеров пользователей вредоносным ПО, так как у них были настроены соответствующие правила в SIEM. Вредоносное ПО позволяло злоумышленникам удаленно получать доступ к компьютерам пользователей и управлять ими.

Зараженные компьютеры были оперативно изолированы из корпоративной сети и излечены. Примечательно, что, как выяснилось в ходе разбирательства инцидента, вредоносное вложение было запущено в том числе сотрудниками служб безопасности.

Случай показательный. Несмотря на то что в банке существуют процедуры повышения осведомленности по вопросам информационной безопасности, проводится обучение персонала, эти меры оказались недостаточно эффективными.

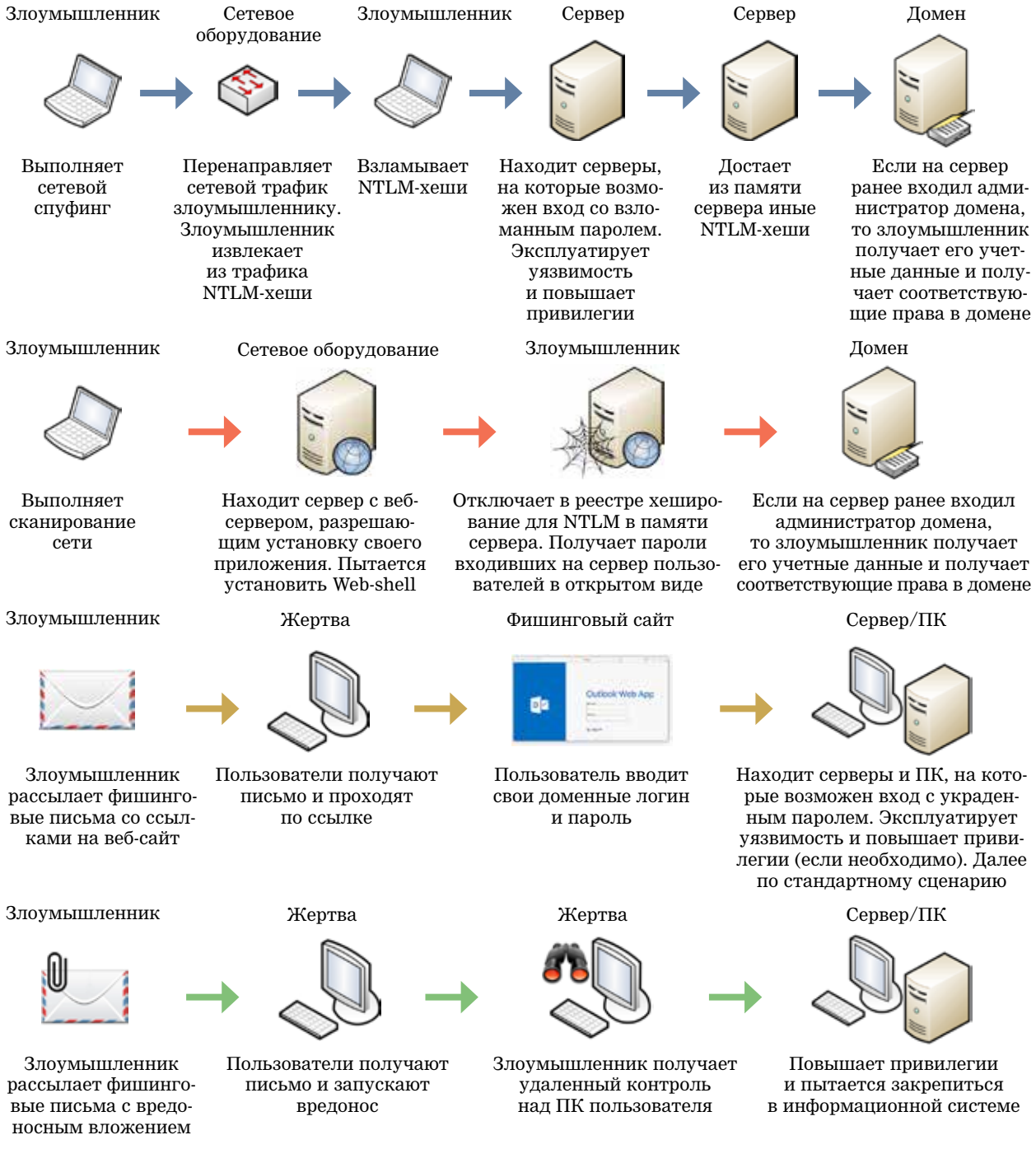
Пример 2

В одной финансовой организации проводились параллельно работы по тесту на проникновение и аудиту процессов менеджмента инфор-

Топ-9 уязвимостей: как справиться с ними при помощи SOC?

Рисунок 2

Варианты векторов атак и шагов злоумышленников



Андрей ГАЙКО

мационной безопасности, в том числе проверка работоспособности действующего SOC. Надо отметить, что в организации был свой отдел мониторинга событий ИБ, но она также пользовалась услугами стороннего SOC. Организация передавала стороннему SOC события со своих систем, SOC проводил их анализ и оперативно отправлял сообщения об обнаруженных инцидентах.

Тестирование на проникновение выявило существенные проблемы в безопасности. Для получения прав доменного администратора пентестеры использовали один из описанных в статье векторов атак. Применялась модель внутреннего нарушителя. Рабочую станцию пентестеров подключили к подсети, в которой размещались пользователи компании. Была создана доменная учетная запись в домене без каких-либо прав.

Пентестеры просканировали доступные из пользовательского сегмента подсети. Обнаружился веб-сервер с установленным на нем веб-сервером Tomcat. Этот веб-сервер давал возможность установить собственное ПО, обратившись к нему на порт 8080. Воспользовавшись этой возможностью, пентестеры установили веб-shell (ПО, исполняемое на веб-сервере и позволяющее выполнять команды ОС сервера).

Как оказалось, веб-сервер Tomcat был запущен под сервисной учетной записью, имеющей системные права, то есть позволяющей выполнять любые команды. Таким образом, пентестеры могли выполнять любые привилегированные команды сервера.

На сервер было установлено ПО, которое позволяло сделать дамп оперативной памяти сервера. Из памяти были извлечены NTLM-хеши. Была проведена успешная bruteforce-атака на эти хеши и получен пароль от учетной записи доменного администратора, так как ранее администратор входил на этот сервер.

После успешной атаки были опрошены сотрудники службы мониторинга. Они не получали от внешнего SOC каких-либо сообщений об этой атаке. Сами сотрудники также не заметили какой-либо странной активности.

Итоговые рекомендации

Конечные цели злоумышленников остаются теми же, что и всегда, — украсть деньги. Однако вектор атак изменился. Еще в 2014 г. мы прогнозировали, что будет расти количество нападений на внутрибанковские системы. Вектор атак продолжит расширяться с клиентов банков на сами банки. Статистика 2015–2016 гг. это подтверждает.

Банки оказались не готовы к такому повороту событий. Показательными были случаи в конце 2015 г. Выходит, что переложить

Топ-9 уязвимостей: как справиться с ними при помощи SOC?

вину за кражу средств на клиента уже не получится. Необходимы серьезная подготовка и решительные действия. Одной только «бумажной» безопасности стало мало. Поэтому специалистам по информационной безопасности в финансовых организациях надо более глубоко погружаться в информационные технологии, проводить их анализ с технической точки зрения и более эффективно организовывать менеджмент ИБ.

На основании всего сказанного мы можем дать следующие рекомендации по повышению эффективности SOC.

На уровне менеджмента ИБ:

— наладить взаимодействие IT и ИБ;

— подразделению ИБ с привлечением подразделения IT провести инвентаризацию информационных активов, систем, прикладного и системного ПО, поддерживать перечни инвентаризации в актуальном состоянии, вести контроль за появлением новых систем и технологий в информационной инфраструктуре;

— специалистам SOC изучать и разбираться в особенностях новых технологий и анализировать их использование с точки зрения информационной безопасности, рассчитывать потенциальные риски и вырабатывать защитные меры;

— разрабатывать документацию для SOC в простой и понятной для всех форме.

На техническом уровне:

— проанализировать указанные атаки, понять, где в ИС, к каким узлам ИС эти атаки могут быть применены;

— определить источники данных, типы событий, с использованием которых данные атаки могут быть предотвращены, превентивно обнаружены и обработаны;

— создать в SIEM соответствующие правила, настроить средства защиты, развернуть и настроить honeypots;

— протестировать защитные меры и правила на тестовом окружении путем имитации атак;

— доработать защитные меры и правила;

— разработать и документировать операционные процедуры, инструкции для персонала первой и второй линий SOC;

— обучить операторов SOC;

— оптимизировать защитные меры, правила выявления атак и процедуры на основании полученного опыта по истечении определенного промежутка времени эксплуатации SOC.