DOI: 10.25728/avtprom.2021.10.10

Проблемы выявления и отражения кибератак на информационные системы

Н.П. Васильев (РТУ МИРЭА), А.В. Фефилов (АО «Перспективный мониторинг»)

Рассмотрена проблема обнаружения и обезвреживания кибератак на информационные системы (ИС), в том числе в реальном времени. Приводятся современные системы обнаружения и предотвращения вторжений (атак) в ИС, включая системы интеллектуального анализа угроз. Описываются некоторые аспекты по обучению специалистов в области информационной безопасности (ИБ), включая on-line-тренинги с использованием инновационного киберполигона Ampire. Система позволяет участникам тренинга как выявлять инциденты информационной безопасности, так и оперативно реагировать на них, закрывая уязвимости в ИС.

Ключевые слова: обнаружение и обезвреживание кибератак, информационные системы, интеллектуальный анализ угроз, киберполигон, обучение.

Введение

Переход к информационному обществу неизбежно привел к тому, что проблемы, с которыми ранее сталкивался достаточно ограниченный круг ИТ-специалистов, приобрели всеобъемлющий характер. Прежде всего, это проблемы информационной безопасности (ИБ), переросшие в глобальные вызовы во всех странах с развитой ИТ-инфраструктурой. Например, согласно [1], киберпреступления будут стоить человечеству 6 трлн. долл. США в 2021 г. (что вдвое больше показателя пятилетней давности), - и это примерно в 1,5 раза больше годового ВВП столь развитой страны, как Германия. В 2019 г. по всему миру кибератаки происходили в среднем каждые 14 с (https://icc.moscow/ru/news).

В Internet представлена масса разного рода сведений о различных киберугрозах (и их последствиях), например, в статье [2] приведен подробный аналитический обзор наиболее «популярных» кибератак. В силу этого не будем углубляться в эту печальную статистику, а перейдем к конкретным вопросам противодействия данной крайне опасной тенденции.

Прежде всего, отметим, что на законодательном уровне также имеет место переосмысление угроз ИБ. Ранее угрозы ИБ рассматривали как нечто статичное и гипотетическое, в контексте «если произойдет, то...», сейчас же требуется обеспечивать безопасность ИС в условиях уже происходящей прямо сейчас атаки. Например, в ФЗ от 26 июля 2017 г. №187-ФЗ «О безопасности критической информационной инфраструктуры РФ», в Статье 2 прямо говорится: *«безопасность критической информационной инфраструктуры - состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак»*. В том же законе (Статья 5) обозначены «силы и средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты».

Данная статья посвящена ряду вопросов в контексте как «*средств*» – инструментов для противодействия компьютерным атакам (КА) и инцидентам (КИ), так и «*сил*» – специалистов ИБ, ответственных за отражение КА.

Как происходит компьютерная атака

Несмотря на многообразие компьютерных инцидентов и атак, все они происходят по достаточно общему типовому сценарию.

1. Злоумышленник (хакер) выбирает подходящую жертву – случайно либо целенаправленно, что происходит гораздо чаще.

2. Хакер выполняет своего рода анализ предметной области: ищет точки соприкосновения атакуемой ИС и Internet (Web-, почтовые, файловые серверы и т.п.), оценивает масштаб (периметр) ИС, определяет ассортимент ПО, установленного в точках соприкосновения, а также выявляет перечень используемых протоколов и портов передачи данных.

3. После этого злоумышленник определяет перечень уязвимостей для выявленного ПО и протоколов ИС и проверяет по этому перечню «крепкость» системы. Важным аспектом является защищенность сред провайдеров услугInternet, в которых функционирует внешняя часть корпоративной сети.

4. Обнаружив присутствие уязвимости, хакер начинает ее эксплуатировать. На этом этапе главной целью, как правило, является проникновение во внутренний периметр ИС, так как в абсолютном большинстве ИС степень защищенности от доступа «изнутри» намного меньше таковой по сравнению с доступом «снаружи».

5. Достигнув успеха (например, проложив туннель между своим, внешним узлом и внутренним узлом ИС), хакер выполняет свое черное дело – скачивает базы данных с

конфиденциальной информацией, внедряет вредоносное ПО, ставит закладки для утечек данных и т.п.

6. После совершения злодейства хакер заметает следы, чтобы защититься от последствий расследования произошедшего инцидента.

Отметим важный тренд в современной информационной среде – организованная киберпреступность. Если раньше в качестве злоумышленников выступали одиночки, то сейчас большинство успешных кибератак выполняются коллективами хакеров, как правило, интернациональными, действующими во всех часовых поясах. Это позволяет вести круглосуточный злонамеренный мониторинг потенциальных жертв и иметь «продвинутые» модели будущих объектов атак (испытательные полигоны) для тщательной проверки на прочность современных аппаратных решений, программных систем и протоколов, не привлекая к себе внимания.

Более того, нынешние злоумышленники профессионально владеют методами социальной инженерии, то есть мягкого, ненавязчивого воздействия на жертв с целью заставить последних выполнить определенные действия, – причем пострадавшие будут свято уверены, что действовали по собственной воле. Например, авторам известны случаи, когда злоумышленники после изучения характера и привычек сотрудников организаций по их публикациям в социальных сетях, посылали жертвам фишинговые (от спецтермина phishing, происходящего от англ. fishing – рыбалка) письма-наживки с содержанием, воспринимавшимся получателями как переписка, связанная с их безобидными хобби: домашние животные, игрушки, рукоделие и т.п. Открыв такое письмо, жертва получает на своем компьютере «черный ход» (backdoor), через который утекает конфиденциальная информация.

Теперь перейдем к рассмотрению основных методов и средств защиты от КА.

Ложные объекты атаки

Ложный объект атаки (ЛОА) (honeypot, горшочек меда) представляет собой модель ИС, предназначенную для привлечения внимания атакующего вместо реальной ИС. В такой модельной ИС значимые конфиденциальные сведения отсутствуют. Очень хорошее, можно сказать, фундаментальное, хотя и устаревшее описание honeypot-приемов дано в [3]; перечень некоторых систем ЛОА (как платных, так и общедоступных) приведен в [4].

Использование ЛОА решает две задачи: во-первых, защитить настоящую ИС, и, во-вторых, провести мониторинг действий атакующего с целью его обнаружения, поиска метода противодействия и т.д. Эффективность ЛОА напрямую зависит от степени ее правдоподобности; к тому же хакеры умеют распознавать известные системы ЛОА по их признакам.

Построение полноценной системы ЛОА фактически удвоит расходы на развертывание ИС: понадобится создать вторую копию ИС, да еще и с правдоподобными (но не соответствующими истине) данными, что представляет собой нетривиальную задачу. Развертывание же упрощенного honeypot'а может иметь обратный эффект: обнаружив ловушку, хакер поймет, что в атакуемой системе есть, что защищать, и умножит свои усилия по взлому, привлекая коллег по ремеслу.

Сетевые экраны

Использование *сетевых экранов* (СЭ) (firewall, Brand Mauer) – классическая технология обеспечения ИБ, направленная на обеспечение доступности вычислительных ресурсов посредством блокировки нежелательного трафика. Среди СЭ выделяют *межсетевые* и *персональные* сетевые экраны; в России действуют достаточно жесткие требования ко всем категориям СЭ, предъявляемые Федеральной службой по техническому и экспортному контролю (ФСТЭК России). Одним из ключевых требований к СЭ является функционирование по принципу «белого списка», то есть трафик, не разрешенный явным образом, будет блокироваться («что не разрешено, то запрещено»).

Работа с СЭ по принципу «белого списка» требует заметных усилий от администраторов по настройке правил фильтрации трафика, но зато гарантирует блокировкулишнеготрафика.Большимподспорьемвработеадминистраторов больших сетей является возможность централизованного управления политиками безопасности (то есть множествами правил фильтрации трафика и трансляции сетевых адресов (NAT).

Системы обнаружения вторжений и атак

Системы обнаружения вторжений (СОВ) (Intrusion Detection System, IDS) – еще одна из классических технологий ИБ. Согласно классификации ФСТЭК России, выделяют СОВ уровня сети (Network IDS, NIDS) и уровня узла (Host IDS, HIDS). Те и другие в свою очередь подразделяются на шесть классов защищенности: от максимального первого, до минимального шестого. Краткая характеристика этих систем.

- *СОВ классов защиты* 1, 2, 3 применяются в ИС, в которых обрабатывается информация, содержащая сведения, составляющие государственную тайну.
- *СОВ класса* 4 применяются в ИС персональных данных (ПДн) 1 класса (медицинские, социальные), ИС общего пользования II класса, а также в ГИС, в которых обрабатывается информация ограниченного доступа, не содержащая сведений, составляющих государственную тайну.
- *СОВ класса* 5 применяются в ИС ПДн 2 класса (идентификационные+ доп. информация).
- *СОВ класса* 6 применяются в ИС ПДн 3 класса (идентификационные) и 4 класса (обезличенные, общедоступные).

ФСБ России также предъявляет свои требования к системам обнаружения атак (СОА). Согласно классификации ФСБ выделяются 4 класса СОА: от максимального уровня (А) до минимального (Г). Если ФСТЭК в своей классификации исходит из целевого назначения СОВ, то ФСБ классифицирует СОА в соответствии с их компонентами: наличие подсистемы управления, контролируемые ресурсы и протоколы, ведение системных журналов и т.п.

Примерами СОА (СОВ), нацеленными на промышленное применение, могут служить системы ViPNet IDS NS и ViPNet IDS HS. Первая из них представляет собой

СОВ (СОА) уровня сети, вторая – уровня узла (хоста); обе системы включают как сигнатурный, так и эвристический анализ событий ИБ. Сигнатурный анализ (СА) основан на поиске в сетевом трафике и в поведении хоста признаков известных угроз ИБ. Базы данных этих сигнатур регулярно пополняются и обновляются специалистами группы компаний «ИнфоТеКС» (https://infotecs.ru). Эвристический анализ (ЭА) основан на поиске аномалий в трафике или поведении системы: в течение определенного периода система самообучается, выстраивая шаблон поведения контролируемой ИС, и как только ее текущее поведение отличается от шаблонного по некоторым пороговым величинам, фиксируется событие ИБ (СИБ). Все системы ViPNet IDS имеют развитую подсистему оповещения о возникших СИБ: от уведомления до интеграции с промышленными SIEM-системами (Security Information and Event Management – управление информационной безопасностью и СИБ).

Отличительной особенностью систем ViPNet IDS NS и HS является возможность централизованного управления посредством комплекса ViPNet IDS MC (management center – центр управления). Такой комплекс ориентирован на крупные организации и позволяет централизованно осуществлять полный цикл управления сетевыми и хостовыми сенсорами: от автоматического обновления сигнатур и правил обнаружения вредоносного ПО до концентрации сведений о СИБ в едином штабе.

Системы интеллектуального анализа угроз информационной безопасности

Основной проблемой всех СОВ (СОА) является то, что они реагируют на одиночные события ИБ, например, обнаружение факта сканирования портов, нештатное применение протоколов, использование хакерских утилит, попыток поиска уязвимостей в ИС и т.п. Таких событий в процессе эксплуатации ИС возникает великое множество, а за поиск реально опасных цепочек событий, приводящих к инцидентам ИБ, когда ИС оказывается под реальной угрозой, отвечает человек – специалист по ИБ. При этом человека ни одна информационная система заменить не может, но потребность в системах интеллектуального анализа угроз ИБ (СИАУИБ) растет с каждым днем. Если ввести в любой поисковой системе фразу «система интеллектуального анализа угроз ИБ», увидим массу ссылок на различные публикации и исследования, а готовых решений на настоящий момент почти нет. Исключением является система ViPNet TIAS (Threat Intelligence Analytics System – система интеллектуального анализа угроз), которая собирает сведения о событиях ИБ с подключенных к ней сенсоров, а именно, систем ViPNet IDS NS и HS. На основе алгоритмов машинного обучения ViPNet TIAS из всей огромной массы СИБ выделяет *цепочки* событий, которые приводят к инциденту ИБ. Если провести аналогию с жизнью, то *событие* подобно *симптому* некоторого заболевания, а *инцидент* – уже само *заболевание*, которое может иметь очень тяжелые последствия. Обнаружив инцидент ИБ (ИИБ), ViPNet TIAS фиксирует этот факт, уведомляя специалистов ИБ различными способами, арсенал которых весьма широк: от простого уведомления до действий в рамках SIEM-системы. Более того, ViPNet TIAS содержит подсистему управления учетными карточками инцидентов ИБ, которая позволяет облегчить процесс их обработки специалистами.

Системы предотвращения вторжений

Данный класс систем (СПВ, IPS – от Intrusion Prevention System, система предотвращения вторжений) представляет собой интеграцию систем обнаружений атак (вторжений) и межсетевых экранов. СПВ содержит автоконфигурируемый СЭ и СОВ (СОА): СОВ регулярно обновляет свою базу сигнатур (БРП – база решающих правил), и при обнаружении в трафике СИБ встроенный файрвол блокирует для источника такого трафика доступ к ресурсам защищаемой сети.

В последние годы СПВ появляются все чаще как в России, так и за рубежом. Хорошим примером такой системы с ограниченным применением для домашнего использования является продукт pfSense, который можно загрузить с сайта производителя (https://www.pfsense.org/download/). По личному опыту использования в домашней сети одного из авторов, можно утверждать, что система хорошо выполняет свою работу, список обнаруженных и блокированных СИБ очень впечатляет. Однако такого рода система не может быть использована для промышленного применения по двум причинам. Первая из них заключается в том, что к такого рода системам в России предъявляются весьма высокие требования, и pfSense, и ей подобные не входят в список сертифицированных ФСТЭК средств защиты информации (СЗИ). Второй же причиной являются лицензионные ограничения производителя, исключающие коммерческую эксплуатацию.

Примером полноценной промышленной системы СПВ может служить продукт ViPNet xFirewall 5, включающий модуль IPS, который обновляется на основе правил, создаваемых специалистами группы компаний «ИнфоТеКС».

Обучение специалистов по информационной безопасности

Ни одна, даже наисовершеннейшая ИС не способна заменить человека. И перечисленные системы суть не более чем сложные и точные инструменты, которые в полной мере способны проявить свои качества только в умелых руках специалиста. В силу этого, проблема обучения квалифицированных кадров в области ИБ сейчас является актуальной, как никогда ранее. Тема настолько обширна и серьезна, что заслуживает отдельной статьи, которую авторы планируют опубликовать в ближайшем будущем, опираясь на свой многолетний опыт в сфере высшего и дополнительного профессионального образования. В данной же работе ограничимся тезисом: как в России, так и за рубежом в настоящее время имеет место серьёзный кадровый дефицит профессионалов в сфере ИБ.

Киберполигон Ampire для обнаружения и ликвидации последствий компьютерных атак в режиме реального времени

Поскольку обучение специалистов по ИБ немыслимо без современных программных и технических средств, потребности в таковых остаются и будут оставаться

на высоком уровне. Более того, в силу высокой изменчивости предметной области (появление все более новых компьютерных атак) такие обучающие системы должны иметь возможность для постоянного пополнения новыми сведениями.

Система Ampire (https://reestr.minsvyaz.ru/reestr/159499/), разработанная компанией "Перспективный мониторинг", входящей в группу ИнфоТеКС, представляет собой программный комплекс, включающий полноценную модель ИС предприятия: в нем содержатся как модели сетевого оборудования, так и виртуальные машины, на которых развернуты информационные ресурсы некоторой абстрактной организации: Web-, FTP- и почтовые серверы, серверы баз данных, контроллеры доменов и т.п. Имеется подсистема «Электронный нарушитель» (ЭН), которая имитирует действия хакера-злоумышленника; ЭН в режиме реального времени проводит атаку по заранее введенному сценарию, взламывая ресурсы ИС. В качестве инструмента для выявления атак используется ViPNet IDS NS 3; взаимодействие обучаемых и системы происходит через Web-интерфейс и посредством удаленного рабочего стола. Система Ampire применяется в учебном процессе в МИРЭА.

Ampire позволяет смоделировать в *реальном времени* работу центра обеспечения безопасности компании (SOC, Security Operations Center). Занятия проводятся под руководством преподавателя; аудитория обучаемых делится на две группы: группа мониторинга (ГМ) и группа реагирования (ГР). Задачей ГМ является выявление событий ИБ, происходящих в результате компьютерной атаки (КА); все члены ГМ равноправны и работают независимо друг от друга. Их единственным инструментом является Web-браузер, посредством которого они получают доступ как к Ampire, так и к ViPNet IDS NS. Задачей ГР является ликвидация последствий КА, а именно, устранение тех уязвимостей в ИС, которые стали предметом КА. Для ГР преподавателем назначается старший группы, функции которого заключаются как в координации работы группы, так и в непосредственном участии в устранении последствий КА.

Работа комплекса Ampire происходит следующим образом.

1. Преподаватель выполняет подготовительные действия: определяет продолжительность тренинга, выбирает сценарий для имитации КА в системе, дает краткую вводную по КА (15 мин), делит аудиторию на ГМ и ГР, назначает старшего ГР, знакомит обучаемых с правилами работы в системе.

2. После этого преподаватель запускает электронного нарушителя; начинается имитация КА. С технической точки зрения это самая настоящая КА, но направлена она не на реальную ИС реальной организации, а на точную модель ИС абстрактной компании.

3. ГМ приступает к работе: каждый член группы с помощью ViPNet IDS NS ищет события ИБ, относящиеся к целевой КА, и формирует карточки инцидентов в среде самой системы Ampire.

4. Преподаватель, в деталях знающий сценарий КА (что делает ЭН, и какие ресурсы ИС затронуты), оценивает карточки инцидентов и выставляет им оценки от 1 до 5 звездочек. Оценка формируется исходя из соответствия карточки вектору атаки и полноты описания ситуации, например, если обнаруженное событие в точности описывает действие нарушителя, содержит вложенный файл с сетевым пакетом (в формате PCAP) и соответствует «взломанному» ресурсу, то выставляется максимум – 5 звезд. Такой способ оценки, в звездах, выбран сознательно – преподаватель обязательно должен подчеркнуть, что это не баллы успеваемости, а степень точности описания события ИБ.

5. По мере появления карточек инцидентов ИБ старший ГР их распределяет среди членов своей группы (в том числе беря часть их себе) для обработки. При этом оценка преподавателя является для него критерием отбора наиболее значимых карточек.

6. Для обработки карточек инцидентов каждый участник ГР (включая старшего) с помощью удаленного рабочего стола получает доступ к виртуальным машинам ИС предприятия. Имея административные полномочия, член ГР находит уязвимое место системы и, опираясь на свои навыки в сфере ИБ, устраняет проблему.

7. Каждый сценарий системы Ampire предполагает устранение трех уязвимостей, изначально они обозначаются красным цветом. Когда уязвимость устранена, ее индикатор становится зеленым. Если же кто-то из ГР просто выключил соответствующую службу или компьютер, то есть заблокировал работу ИС или ее части, индикатор уязвимости становится синим. Целью киберучений является полноценное устранение всех трех уязвимостей (три зеленых индикатора) за отведенное на тренировку время.

8. По завершению сценария преподавателем проводится детальный разбор КА и дается оценка достигнутым результатам.

9. В зависимости от времени, отведенного на мероприятие, преподаватель может запустить следующий сценарий КА. При этом члены ГМ и ГР меняются местами.

Отметим, что система постоянно пополняется новыми сценариями КА, что позволяет на ее основе проводить не только разовые мероприятия, но и продолжительные учебные курсы. Система Ampire применяется в тренингах, проводимых в рамках конференций и выставок, а также в ряде учреждений высшего и дополнительного профессионального образования.

Личный опыт авторов свидетельствует об очень высокой заинтересованности обучаемых: нами многократно проводились как очные, так и дистанционные киберучения на базе комплекса Ampire, и участники давали происходящему неизменно высокие оценки.

Заключение

Конечно, в рамках одной статьи невозможно дать детальное описание, а тем более точные рецепты для обеспечения защищенности информационных систем.

Тем не менее, авторы постарались раскрыть ряд важных аспектов в данной области и сделать некоторые выводы, а именно:

• современный мир ставит перед всеми нами постоянно растущий ряд вызовов в области информационной безопасности, и от них нам нигде и никак не укрыться. Мы обязаны на них реагировать, а еще лучше, действовать с упреждением;

• число компьютерных атак растет и будет расти;

• имеется насущная необходимость в разработке и совершенствовании средств защиты информации: СЭ, СОВ (СОА), системах предотвращения вторжений, системах интеллектуального анализа и т.п.;

• российские программные и технические решения в области ИБ не только имеются, но и находятся высоком уровне, не уступая зарубежным аналогам (а порой и превосходя их);

• необходимо прививать и совершенствовать знания, умения и навыки в области ИБ – при чем для всех: от школьников и до высококвалифицированных специалистов в области ИБ. Это требует концентрации усилий всех субъектов образовательной среды: от школ до вузов и организаций дополнительного профессионального образования.

Список литературы

1. *Steve Morgan*. Cybersecurity labor crunch to hit 3.5 million unfilled jobs by 2021 [Электронный ресурс]. https://www.csoonline.com/article/3200024/cybersecurity-labor-crunch-to-hit-35-million-unfilled-jobs-by-2021.html
2. Актуальные киберугрозы: итоги 2019 г. https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2019
3. *Lance Spitzner*. Honeypots: Tracking Hackers. Addison Wesley, 2002.
4. Honeypots Solutions. https://web.archive.org/web/20090308063216/ http://www.tracking-hackers.com/solutions/

Васильев Николай Петрович *- канд. техн. наук, доцент, доцент кафедры КБ-1 «Защита информации» МИРЭА – Российского технологического университета (РТУ МИРЭА),*

Фефилов Александр Валерьевич *– старший специалист информационной безопасности АО «Перспективный мониторинг».*

И БЕЗОПАСНОСТЬ МОЖЕТ БЫТЬ НА АУТСОРСЕ

А.С. Филатов (Компания Tet)

Для обнаружения и устранения угроз в области информационной безопасности на предприятиях создаются центры управления безопасностью либо такие услуги предоставляются по подписке через аутсорсинг. Рассмотрены плюсы и минусы каждого из этих решений.

Ключевые слова: аутсорсинг, кибербезопасность, центры управления безопасностью, промышленные предприятия.

Утечки данных, заражение вредоносным ПО и кибератаки стали привычным явлением как для больших, так и для малых организаций по всему миру. Так, число инцидентов, связанных с программами-вымогателями, в производственном секторе увеличилось на 156% в период с первого квартала 2019 г. по первый квартал 2020 г.

Раньше ситуация была иная — компаниям промышленного сектора не нужно было подключать свои системы управления производством (Industrial control systems — ICS) к Internet. Это означало полную защиту от внешних угроз и не требовало ничего, кроме контроля за физическими процессами.

Теперь большинство компаний в том или ином виде имеют выходы в «большой» Internet, а значит и потребность в кибербезопасности выросла до уровня бизнеса из любой другой сферы. Для минимизации времени простоя, которое может быть вызвано атакой на предприятие, игрокам производственного сектора необходимо отслеживать и анализировать огромный объем данных в реальном времени.

Обнаружение и устранение угроз до того, как они вызовут какие-либо негативные последствия, — ежедневный приоритет для ИТ-команд. Однако, даже несмотря на усилия высококлассных специалистов по информационной безопасности, защититься от хакеров получается далеко не всегда.

Приходится принять тот факт, что добиться 100% безопасности невозможно ни при каких обстоятельствах. Можно лишь уменьшить риски и держать ситуацию под постоянным контролем. Многие ИТ-отделы достигают этих целей путем внедрения в свою деятельность центра управления безопасностью (security operations centre — SOC). Он может быть как частью самой компании, так и услугой по подписке.

Как можно управлять безопасностью?

Основная функция центра безопасности — круглосуточный мониторинг инфраструктуры с целью обнаружения, предотвращения или реагирования на киберугрозу, а затем проведение комплексного расследования. Команды SOC отвечают