Секция «Актуальные проблемы информационной безопасности», научный руководитель – Ищукова Е.А., канд. техн. наук, доцент

МУЛЬТИФАКТОРНАЯ АУТЕНТИФИКАЦИЯ КАК ФАКТОР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ АТТЕСТАЦИИ СТУДЕНТОВ

Инджиев А.Н., Горяев В.М.

Калмыцкий государственный университет, Элиста, e-mail: goryaeff@rambler.ru

В ходе своих исследований на кафедре ИТ мы разрабатываем программно- аппаратный комплекс, который позволяет достоверно идентифицировать студента. В современных условиях средние и высшие учебные заведения хотят продвинуть качество услуг для своих сотрудников и студентов в цифровом образовательном пространстве. В последнее время мы наблюдаем увеличение интенсивности использования новых интернет- приложений в учбеных заведениях, что ведет к многочисленным сопутствующим проблемами.

Безопасный доступ к приложениям электронного обучения и внутренним сетям крайне важен, из-за конфиденциального характера данных. Цифровые данные администрации, сотрудников и студентов должны быть защищены. Именно поэтому все больше вузов признает важность продвинутых решений при идентификации. Специалисты по безопасности давно рекомендуют менять опасные статические пароли на более безопасные динамично произведенные одноразовые пароли. Они могут только использоваться однажды, таким образом устраняя несанкционированный доступ к конфиденциальным данным.

Проблемы, которые могут возникнуть при плохом уровне безопасности:

1. Кража персональных данных
2. Несанкционированный доступ к данным
3. Мошенничество в онлайн
4. Фишинг – вид интернет-мошенничеств и т.д.

Данная работа посвящена «сильным» решениям для идентификации в образовательном процессе для колледжей, университетов, школ. Сильная идентификация предлагает продвинутую безопасность для сотрудников, преподавателей, продавцов и студентов.

Данная работа была направлена на обеспечения «сильной» верификации в процессе различных аттестаций студентов и курсантов. Для ускорения процесса авторизации можно воспользоваться специальным сформированный одноразовым QR-кодом, соотнесенным с конкретной группой или преподавателем и распознанным перед видеокамерой терминала. QR-код можно получить при выборе группы, он отображается на экране и его можно сфотографировать на смартфон, также его можно будет получить с любого компьютера внутренней сети университета (через логин и пароль) и распечатать на принтере.

Компьютер преподавателя должен быть оснащен web-камерой и функцией распознавания лиц. На компьютере формируется QR-код для экзамена. Студент, вызванный на экзамен подходит с этим графическим кодом к считывающему устройству (смартфон или компьютер), затем QR-код отсылает на определенную страницу университетского сайта, где идет распознавание экзаменуемого и в случае успешной завершения процесса выдается квиток с билетом (в противном случае придется выполнять документоориентированное опознавание лица). В общем случае, обладая уникальным QR-кодом можно получить доступ к режиму обучения распознаванию лиц для более лучшей идентификации.

Наиболее интересно использовать мультифакторную аутентификацию для студентов заочной формы обучения и, особенно, для обучаемых в рамках дистанционного обучения, когда нет уверенности в том, что экзамен сдает зарегистрированный в вузе учащийся, а не проплаченный двойник. Для дистанционного обучения используется тот же алгоритм: студент во время сессии заходит в свой личный кабинет и получает сгенерированный QR-код, затем продемонстрировав камере этот код ожидает распознавания личности несколько секунд для доступа к экзамену. Время от времени компьютер сверяется с базой открытой QR-кодом для того, чтобы можно было достоверно выявить зловредные манипуляции в процессе экзамена.

МОНИТОРИНГ СОБЫТИЙ И ОБНАРУЖЕНИЕ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ИСПОЛЬЗОВАНИЕМ SIEM-СИСТЕМ

Канев А.Н.

Университет ИТМО, Санкт-Петербург, e-mail: ta1ler93@mail.ru

Обеспечение информационной безопасности (ИБ) является важной задачей для различных организаций. Выполнение этой нетривиальной задачи требует значительных финансовых и трудовых затрат. Важно понимать, что эти затраты сделаны впустую, если система защиты информации при этом действует недостаточно быстро и продуктивно. Поэтому в последнее время все актуальнее становится проблема мониторинга событий ИБ (далее – событий), а также обнаружение и обработка возникающих инцидентов ИБ (далее – инцидентов) в минимальные сроки.

Ключевым понятием в рассматриваемой области является «событие информационной безопасности», для которого в современном законодательстве принято следующее определение:

Событие – идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нарушение политики ИБ или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности [1, 2].

Мониторинг событий производится на основе данных, полученных из различных источников, к которым относятся:

- IDS/IPS-системы;
- средства антивирусной защиты;
- журналы событий;
- сканеры уязвимостей;
- DLP-системы,
- сетевое оборудование;
- прочие источники.

Количество источников событий возрастает с ростом организации, то есть с ростом числа серверов, автоматизированных рабочих мест, сетевого оборудования и прочих объектов инфраструктуры. Информация из различных источников хранится раздельно, имеет разные форматы, и, как следствие, никак не связана между собой. Для крупных организаций затруднительно обрабатывать достаточно быстро и эффективно такой поток событий ограниченным персоналом подразделения, ответственного за мониторинг.

Это проявляется в низкой скорости выполнения анализа событий, его качестве и невыявлении взаимосвязей между событиями, являющихся симптомами инцидента.

Проблемы мониторинга событий негативно влияют на выявление инцидентов.

Инцидент – появление одного или нескольких нежелательных или неожиданных событий, с которыми связана значительная вероятность компрометации бизнес-операций и создания угрозы ИБ [1].

Инцидент – любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность [2].

Инцидент – событие или комбинация событий, указывающая на свершившуюся, предпринимаемую или вероятную реализацию угрозы ИБ, результатом которой являются:

• нарушение или возможное нарушение работы средств защиты информации в составе СОИБ организации БС РФ;

• нарушение или возможное нарушение требований законодательства РФ, нормативных актов и предписаний регулирующих и надзорных органов, внутренних документов организации БС РФ в области обеспечения ИБ, нарушение или возможное нарушение в выполнении процессов СОИБ организации БС РФ;

• нарушение или возможное нарушение в выполнении банковских технологических процессов организации БС РФ;

• нанесение или возможное нанесение ущерба организации БС РФ и (или) ее клиентам [3].

Определения выше различаются, но все они, так или иначе, указывают на причинение негативных последствий процессу, информационной системе, организации в результате возникновения инцидента. Таким образом, своевременное выявление инцидента минимизирует потери организации.

В условиях децентрализации информации о событиях из многих источников обнаружение инцидента становится сложной и не всегда решаемой задачей. После выявления инцидента необходимо идентифицировать пострадавшие активы, понять причины инцидента, оценить его степень тяжести, приоритет, предпринять меры по реагированию. При выполнении этих операций исполнители зачастую сталкиваются с той же проблемой разрозненности источников информации. Это проявляется в ненадлежащем реагировании или его отсутствии, что влечёт за собой убытки организации.

SIEM-система позволяет избежать указанных выше проблем. Она решает задачи по сбору и хранению информации из различных источников, анализу поступающих событий, их корреляции и обработке по правилам, обнаружению инцидентов, их приоритезации и автоматическому оповещению. Кроме того, SIEM-системы часто имеют возможность проведения проверки на соответствие стандартам.

Типовая структура SIEM-систем:

• агенты – устанавливаются на информационную систему и передают данные с нее на сервер, в состав агентов могут включаться модули для преобразования данных;

• сервер-коллектор – собирает события от множества источников;

• сервер-коррелятор – собирает и обрабатывает информацию от коллекторов и агентов;

• сервер баз данных – хранит журналы событий.

SIEM-система собирает информацию из различных источников с помощью агентов и серверов-коллекторов в централизованное хранилище данных, что позволяет впоследствии анализировать события в целом. Также это позволяет избежать разрозненной и, в подавляющем числе случаев, неконтролируемой конфигурации средств анализа событий. Негативным моментом такого построения системы является возрастание нагрузки на сеть организации.

После сбора информации SIEM-система начинает анализ событий ИБ, требующийся для обнаружения инцидента. Для этого применяются 2 основных метода корреляции: сигнатурный (т.е. на основе правил) и бессигнатурный, определяющий аномальное поведение информационной системы. По результатам анализа SIEM-система показывает выявленные инциденты ИБ.

Для того чтобы SIEM-система эффективно выполняла свои задачи в конкретной организации, требуется правильная конфигурация корреляционных механизмов и постоянная их модификация. Вследствие этого SIEM-системы начинают окупать себя значительно позже ее внедрения, особенно при применении бессигнатурных методов корреляции, которые требуют накопления статистических данных. Настройкой SIEM-системы организации, как правило, занимается эксперт, прошедший специальные курсы и имеющий определённый опыт в этой области.

Кроме основной задачи по мониторингу событий и обнаружению инцидентов на основе данных о критичности активов организации и опасности угрозы SIEM-системы могут приоритезировать инциденты, автоматически оповещать об инциденте, выдавать заранее подготовленные рекомендации по немедленному реагированию на инцидент, хранить данные об инциденте для последующего расследования.

На данный момент на рынке SIEM-систем можно выделить следующие продукты:

• HP ArcSight;
• McAfee Nitro;
• IBM QRadar;
• Splunk SIEM;
• RSA Security Analytic;
• LogRhythm.

Применение SIEM-системы не является обязательным при построении комплексной системы защиты информации и во многих случаях нецелесообразно. Основным заказчиком таких систем являются крупные организации, в которых требуется непрерывный контроль за обеспечением ИБ и журналирование связанных с этим событий.

В заключение хотелось бы отметить, что SIEM-системы – это развивающийся продукт, функциональные возможности которого со временем расширяются.

Список литературы

1. ГОСТ Р ИСО/МЭК ТО 18044–2007 »Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности», 2 стр.

2. ГОСТ Р ИСО/МЭК 27001–2006 »Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности – Требования». – 2 с.

3. СТО БР ИББС-1.0-2014 »Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения». – 9 с.

ОБЗОР МЕТОДИК ПРОВЕДЕНИЯ ПРОВЕРОК НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, ПРЕДСТАВЛЕННЫХ В РОССИЙСКИХ И ЗАРУБЕЖНЫХ НОРМАТИВНЫХ ДОКУМЕНТАХ

Никифорова К.А.

Университет ИТМО, Санкт-Петербург,
e-mail: nikiforova.k.a@yandex.ru

Управление соответствием системе требований нормативных документов в области информационной безопасности (далее ИБ) – процесс, направленный на