Шаханова М.В., Малый М.Г., Шаханова Д.С. Автоматизация процессов информационной безопасности // Международный журнал информационных технологий и энергоэффективности. – 2022. – Т. 7 № 4(26) часть 1 с. 67–74

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056.5

АВТОМАТИЗАЦИЯ ПРОЦЕССОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

[1]Шаханова М.В., Малый М.Г., Шаханова Д.С.
Морской государственный университет имени Г.И. Невельского, Владивосток, Россия (690003, г. Владивосток, ул. Верхнепортовая, 50а), e-mail: [1]marinavl2007@yandex.ru

В текущих условиях цифровизации, компании, учреждения и организации вынуждены осуществлять обработку и хранение персональных данных на цифровых носителях, создавать data base типа информационных систем персональных данных (ИСПДн) и оперировать ими. Из чего следует, что возникает необходимость в защите баз данных от утечек наиболее релевантным способом. В данной статье мы разберем какие существуют действующие концепции и вынесем на рассмотрение наиболее оптимальный.

Ключевые слова: автоматизированная защита информации, защита баз данных, коммерческая цифровая безопасность, системы защиты данных, эшелонированная защита данных, automated information protection, database protection, commercial digital security, data protection systems, data protection in depth.

AUTOMATION OF INFORMATION SECURITY PROCESSES

[1] Shakhanova M. V., Malyi M.G., Shakhanova D.S.
Maritime State University named after G.I. Nevelskoy, Vladivostok, Russia (690003, Vladivostok, Verkhneportovaya str., 50a), e-mail: [1]marinavl2007@yandex.ru

In the current conditions of digitalization, companies, institutions and organizations are forced to process and store personal data on digital media, create a data base such as personal data information systems (ISPD) and operate with them. From which it follows that there is a need to protect databases from leaks in the most relevant way. In this article, we will analyze what existing concepts exist and submit the most optimal one for consideration.

Keywords: automated information protection, database protection, commercial digital security, data protection systems, data protection in depth, automated information protection, database protection, commercial digital security, data protection systems, data protection in depth.

Что же нам известно о методах защиты информации с помощью ресурсов корпоративных систем защиты, предусмотренных действующим законодательством?

Во-первых, следует разобраться в вопросе внутренней безопасности [1-3], в частности, чем обуславливаются утечки информации и какие основные угрозы краж интеллектуальной собственности компании существуют и почему компании выбирают основным стратегическим направлением развитие именно информационную безопасность, выделяя на развитие данной отрасли значительную часть своего бюджета.

Одним из факторов опасности является то, что нарушители могут быть не только внешние, не имеющие легитимного доступа к объекту защиты, но и внутренние, то есть сотрудники и руководители компании, а также юридические лица, которые в виду каких-либо

договоров имеющие доступ к атакуемым активам. И в зависимости от того, какие именно были нарушители, разнятся методы борьбы с ними.

И если внутренние угрозы практически полностью нивелируются действующим законодательством РФ [5] (а именно, достаточно подписания типового договора «О неразглашении» или «Коммерческой тайне», чтобы сотрудник опасался передачи информации в третьи руки), то с внешними угрозами все обстоит несколько иначе. Для внутренних – это ещё и технические (DLP – предотвращение утечек информации, управление учётными данными, в том числе. для борьбы с попавшими в локальную вычислительную сеть внешними атакующими), физические (система контроля и управления доступом, Closed Circuit Television), организационные.

И всё же подавляющее большинство направлении ИБ в сфере корпоративной защиты рассчитаны именно на внешние угрозы – антивирусное программное обеспечение (далее – ПО), системы авторизации и контроля доступа, а также системы идентификации пользователя по биометрическим характеристикам.

Предпринимать меры по защите своих ИСПДн и устанавливать ПО, отвечающее требованиям Федеральному закону РФ «О персональных данных», должны любые компании, которые так или иначе обрабатывают персональные данные [7, 8] (далее – ПДн).

Основной проблемой на данный момент является передача ПДн между предприятиями и третьими сторонами для последующего коммерческого использования. Таким образом, утечки информации угрожают безопасности личной жизни и становятся фактором, влияющим на социальную защищенность.

С другой стороны, все чаще крупные компании выбирают для сохранения приватности данных модель Defence In Depth (модель глубоко эшелонированной защиты), что является немаловажным фактором в развитии всей сферы информационной безопасности, позволяющую обеспечить многоуровневую защиту данных.

Остановимся на данной модели, наиболее популярной и рассмотрим ее поподробнее.

- Модель рассчитана на защиту информации, которая имеет для компании коммерческую значимость, а также ту информацию, безопасность которой компании необходимо обеспечить.
- Всего подразделяют 7 уровней защиты (Процедуры ИБ → физический периметр → сетевой периметр → внутренняя сеть компании → рабочее место сотрудника → программы и компоненты ПО → непосредственно данные)
- Непосредственно уровень данных может быть защищен шифрованием, разграничением доступа, специализированными DLP системами (контроля утечек данных).
- Защита программных продуктов обуславливается введением перечня разрешенных и запрещенных в компании программ, парольная политика и своевременное обновление брандмаузеров.
- На рабочее место сотрудников устанавливаются все новейшие обновления (обращая особое внимание на security updates), в принудительном порядке отключаются все ненужные службы.
- На уровне внутренней сети производится сегментирование – разделение сети на невзаимодействующие между собой сегменты, либо же взаимодействующие по строго регламентированным правилам. Применение IPsec – набор протоколов для

обеспечения защиты данных, передаваемых по протоколу IP, т.е. шифрование сетевого трафика. В том числе систем обнаружения вторжений – IPS/IDS или системы предотвращения вторжений, которые отличаются наличием атакующего модуля.

- Если рассматривать уровень сетевого периметра, то самыми распространенным ПО будет Firewall – фильтрующий трафик; создание DMZ-сегментов, доступ к которым повсеместен, благодаря чему разграничиваются внешние и внутренние информационные сервера компании; распространены PROXY-сервера, осуществляющие контроль доступа сотрудников за пределы корпоративной сети; разумеется, DLP-системы, проверяющие весь исходящий интернет-трафик на разглашение информации.
- К уровню физического периметра относятся все физические средства защиты (т.к. охранники, заборы, камеры наблюдения и пр.).
- Последним же уровнем является разработка политики безопасности и процедуры реагирования на кризисные ситуации, а также дополнительные меры в виде обучения сотрудников азам компьютерной грамотности и информационной безопасности.

Таким образом, можно прийти к выводу, что данная модель является на текущем этапе развитии сферы ИБ наиболее рентабельной для ее применения компаниями.

В том числе, когда речь заходит о информационной безопасности в компаниях / на предприятиях, первым делом поднимается вопрос об автоматизации данного процесса.

Зачем же она нужна? Довольно простой ответ на этот вопрос – это недостаток человеческих ресурсов и востребованность в перманентной защите данных, что непосредственно человеческий ресурс обеспечить не может.

Количество нормативной документации в области защиты информации очень велико. Большая часть процессов регламентирована [6], выделяются направления для защиты, увеличивается количество задач по мерам для обеспечения соответствия требованиям по защите информации и проведению оценки соответствия.

Перед автоматизацией стоит поговорить о задачах, стоящих перед сотрудниками отдела безопасности – это сбор и анализ данных о текущем состоянии безопасности, распределение ответственности, оценка и управление рисками, разработка и внедрение защитных мер и механизмов контроля, управление инцидентами, мониторинг введенных систем.

Часть из этих задач можно и нужно делегировать. Причины необходимости автоматизации процессов информационной безопасности кроются в нехватке квалифицированных специалистов, при большом спросе. Неоднородность системы обеспечения информационной безопасности является причиной возникновения множества конфликтов, событий и оповещений на них. Анализ и реагирование на них затрачивает ресурсы отдела. Автоматизация должна решать рутинные задачи, освобождая специалистов для более сложных или необычных задач.

Какие же процессы ИБ можно автоматизировать? Например, валидацию – принятие решения специалистом по ИБ, существенна ли угроза и как ее проще устранить, т.е. процесс обработки инцидентов. Сюда же входят оповещения об инцидентах, процессы реагирования на внешние кибератаки, которые занимают длительное время.

На практике необходимости автоматизации возникает, когда появляется крупная проблема, которую необходимо решить специалисту, но он занят рутинными задачами,

которые возможно передать на автоматическую обработку. Специалисту необходимо обрабатывать различные события, но определение приоритета этих событий можно передать на автоматизацию, таким образом специалист сфокусирован на приоритетной задаче, а не на расстановки приоритета задач или решении всех задач подряд.

Не менее важной причиной необходимости автоматизации является уменьшение влияния человеческого фактора на появление ошибки, так как человек может устать, а машина нет.

Одним из необходимых критериев для возможности введения в эксплуатацию автоматизированных процессов является налаженная работа отдела информационной безопасности.

Плюсы автоматизированных процессов.

- Главный – это уменьшение рисков, ввиду уменьшения влияния человеческого фактора.
- Уменьшение времени простоя в случае возникновения инцидента.
- Повышается управляемость процессами связанными информационной безопасностью, а также повышается эффективность.
- Благодаря переводу квалифицированных сотрудников с рутинных задач на сложные происходит оптимизация затрат.

Также, необходимо заметить, что популярность автоматизации процессов информационной безопасности главным образом связана с ростом числа рисков, инцидентов ИБ увеличиваются изо дня в день. Прогрессирующие число атакующих понимают детально принципы работы организаций, которые подвергаются атакам. Также появились более совершенные средства, методы для организации вторжений, "эксплойтов" направленных на получение конфиденциальной информации, мошеннических действий и информации ограниченного доступа.

Процессы информационной безопасности, которые возможно автоматизировать обширны, одним из таких является возможность получения специалистом контекста без ручного разворачивания всей цепочки. Системы IRP (Incident Response Platform) дают возможность выполнить ряд рутинных операций по сбору дополнительной информации, осуществить неотложные действия по сдерживанию и устранению угрозы, восстановить атакованную систему, оповестить заинтересованных лиц, а также собрать и структурировать данные о расследованных инцидентах информационной безопасности. Существуют различные виды автоматизации, разберем на примере атаки хакеров, автоматизация может дать понять специалисту об атаке и дать возможность блокировки несанкционированного проникновения, или автоматизированный процесс может сам перекрыть несанкционированный доступ.

Одним важных факторов успешной автоматизации является простота использования продукта, т.е. в после введения в эксплуатацию автоматизации не возникла необходимость найма нового специалиста, который работает только с продуктом автоматизации. Конечный вариант продукта должен быть интуитивно понятен и ускорять работу, а не замедлять её.

Для простоты понимания разделим автоматизацию на два вида:

Автоматизация не инвазивных процессов. То есть автоматизация процессов, которые активно не влияют на работу остальных процессов, это сбор данных для контекста для специалиста, расстановка приоритета задачи и т.д.

Автоматизация инвазивных процессов. То есть автоматизация процессов, которые активно влияют на работу системы, к примеру, это изоляция несанкционированного входа в систему, удаление файлов или учетной записи пользователя и т.д.

Не смотря на все плюсы автоматизации есть сегменты работы, которые невозможно автоматизировать, в виду их повышенного уровня важности для работы всей системы, это больше относится к процессам инвазивного характера. Поэтому автоматизация должна идти постепенно. Сначала в компании должны ввести в эксплуатацию не инвазивные процессы, а после, инвазивные.

Отельным пунктом необходимо выделить индустриальные компании, так как в виду повышенных рисков, в том числе и для жизни и здоровья людей, автоматизацию, на данный момент, рекомендуют проводить лишь для инвазивных процессов.

Вопросы информационной безопасности стоят в наше время перед множеством компаний, в крупных компаниях существуют собственные отделы информационной безопасности. Появляется вопрос, стоит самой компании произвести автоматизацию, или отдать это на аутсорсинг? [4]

Из плюсов собственной автоматизации можно выделить доскональное знание автоматизирующими принципов работы конкретного отдела и его нюансов.

Однако стоит отдать стоит вопрос создания автоматизированной системы компании, которая специализируется на них, в виду большего опыта в сфере, а также умения решать проблемы, возникающих при создании и интеграции такого процесса в работу.

Основные задачи, которые должна решать автоматизированная система [9]:

1. Автоматизация процессов управления информационной безопасности.
2. Мгновенный контроль состояния рисков информационной безопасности для руководства.
3. Создание и поддержание актуальной базы учёта активов и бизнес-процессов компании.
4. Классификация мер по защите информации и обработки инцидентов.
5. Управление уязвимостями, обнаруженными в ходе анализа защищённости активов компании.
6. Мониторинг изменений состояния в соответствии с внутренней политикой компании и требованиями стандартов.
7. Поддержка руководства в принятии решений по стратегическому развитию ИБ в организации.

Главная проблема внедрения автоматизации в абсолютное большинство компаний заключаются в том, что не существует общепринятого стандарта представления данных. То есть, для автоматизации, в первую очередь необходимо привести данные к стандартному виду, хотя бы внутри одной компании.

Вторая проблема проистекает из первой, недостаточно данных для создания сценария автоматизации, что уменьшает её пользу в конечно итоге или даже дает отрицательный эффект в скорости работы отдела.

Проблемой повсеместного введения автоматизации служит опасность к атакам на саму систему автоматизации, так как получив управление над ней, можно спокойно управлять всей системой. Следовательно, появляется необходимость в защите этой системы.

Автоматизировать всё это можно различными способами, к примеру core-системы.

1. Система управления логами.
2. Система анализа логов.
3. Система проектирования и автоматизации playbook по реагированию.
4. Система, помогающая работать с threat intelligence.

Из всего этого следует, что автоматизация это не одна программа, а целый комплекс, что может быть слишком сложным для конечного пользователя. Следовательно, мы упираемся в простоту использования продукта, система автоматизации должна быть простой.

Автоматизация большого количества смежных процессов реагирования на инциденты используются системы SOAR (Security Orchestration, Automation and Response), платформы оркестрации, автоматизации и реагирования на инциденты в сфере информационной безопасности. В нём существует следующий функционал [10, 11].

1. Выполнение действий по реагированию.
2. Визуализация, отчетность, аналитика, логирование выполненных действий по реагированию, ведение базы.
3. Возможность совместной работы группы аналитиков над инцидентами.
4. Возможности по обработке данных киберразведки.
5. Возможности по обработке Big Data (структурированные и неструктурированные данные огромных объёмов), механизмы машинного обучения для автоматизации действий и помощи в принятии решений при реагировании на инциденты.

Большая часть вопросов по автоматизации применима к большим корпорация, для более мелких предприятий сама подготовка к введению автоматизации может стать непреодолимым барьеров для этого. В особенности необходимость SIEM (класс программных продуктов, предназначенных для сбора и анализа информации о событиях безопасности) системы, чьё введение и эксплуатация слишком дороги. На данный момент часть компаний, занимающихся автоматизацией, работают и с отсутствием SIEM систем.

Перейдем к новым функциям, которые добавляют к программам для автоматизации. Так как данная сфера относится к информационным технологиям она развивается стремительно быстро. Теперь автоматизированный процесс имеет возможность обучаться в процессе своей работы благодаря технологиям машинного обучения и возможностям искусственного интеллекта. К примеру, он помогает в решении задачи выбора верное срабатывание или нет, сама программа автоматизации, благодаря машинному обучению, может дать некоторую оценку, помогающую в принятии решения.

Главной проблемой машинного обучения является её узкая специализация. То есть, созданная нейросеть умеет только то, для чего её создали, поэтому нейросеть обученная классифицировать события с сетевых сенсоров и выявлять компьютерные атаки на сетевое оборудование не способна работать с мобильными устройствами. И так с каждой проблемой, необходимо будет создавать каждый раз новый продукт и заново его обучать.

Из этого вытекает другая проблема, это нехватка данных для обучения. То есть, нейросеть обучили на одних данных, а на деле она должна будет работать на других, что может на деле вместо уменьшения рутинной работы только добавить её, так как она обучена на других данных.

Одной из проблем вытекающей из самой сути нейросети является неполное знание почему она решила именно так.

Помимо минусов у машинного обучения есть и плюсы, при этом существенные именно в сфере информационной безопасности – это выявление неочевидных для человека закономерностей.

Реальные кейсы успешного применения искусственного интеллекта для автоматизации в плане ускорения, а не улучшения – это когда к сотруднику-аналитику попадает алерт (программируемое оповещение о каком-либо событии), а он на основе него принимает решение, а программа обучается на этом решении. Анализируя сам алерт, его ключевые свойства и взаимосвязи в нём и как они связаны с принятием решения, программа может подсказывать с какой вероятностью это false positive. Этот вариант убирает или минимизирует её главные недостатки, так как она обучается на актуальных данных, она работает именно с тем что нужно.

Будущее автоматизации. Большинство экспертов сходятся во мнении, что существуют несколько принципов, которых будут в будущем придерживаться в разработке систем автоматизации. Это в первую очередь простота, максимально понятные интерфейса, где от пользователя будут просить лишь, согласится или отклонить. Вторым столпом будет увеличение данных при создании контента. Так же в след за увеличением автоматизированных процессов, в сфере информационной безопасности, увеличится необходимость в стандартизации всех процессов, для возможности самой автоматизации.

В данный момент автоматизация процессов просто необходима, так как количество атак растет, растёт их изощренность, поэтому специалисты должны быть разгружены для выполнения тех задач, которые машины, на данный момент, выполнить неспособны. Это сделает систему более отказоустойчивой и надежной.

Список литературы

1. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2008.
2. Петрыкина Н. И. Правовое регулирование оборота персональных данных. Теория и практика. — М. : Статут, 2011.
3. Савельев А. И. Научно-практический постатейный комментарий к Федеральному закону «О персональных данных». — М. : Статут, 2017.
4. Талапина Э. В. Защита персональных данных в цифровую эпоху. Российское право в европейском контексте // Труды Института государства и права РАН. — 2018. — Т. 13. — № 5.
5. Федеральный закон «Об информации, информационных технологиях и защите информации» № 149 — ФЗ от 27 июля 2006 года;
6. ГОСТ Р 6.30-2003 «Унифицированная система организационно-распорядительной документации»;
7. ГОСТ Р 7.0.8.-2013 "Делопроизводство и архивное дело — Термины и определения";
8. Доктрина информационной безопасности;
9. Астахова Л.В. Теория информационной безопасности и методология защиты информации: методическое пособие / Л.В. Астахова. – Челябинск: Изд-во ЮУрГУ, 2007. – 359 с.;
10. Юдин, Э.Г. Методология науки. Системность. Деятельность / Э.Г. Юдин. – М.: Эдиториал УРСС, 1997. – 246 с.;

11. Боровский А. С., Ряполова Е. И… Построение модели системы защиты в облачных технологиях на основе многоагентного подхода с использованием автоматной модели

References

1. Basic model of personal data security threats during their processing in personal data information systems (extract). FSTEC of Russia, 2008.
2. Petrykina N. I. Legal regulation of the circulation of personal data. Theory and practice. - M. : Statute, 2011.
3. Saveliev A. I. Scientific and practical article-by-article commentary on the Federal Law “On Personal Data”. - M. : Statute, 2017.
4. Talapina E. V. Protection of personal data in the digital era. Russian law in the European context // Proceedings of the Institute of State and Law of the Russian Academy of Sciences. - 2018. - T. 13. - No. 5.
5. Federal Law "On information, information technologies and information protection" No. 149 - FZ of July 27, 2006;
6. GOST R 6.30-2003 "Unified system of organizational and administrative documentation";
7. GOST R 7.0.8.-2013 "Office work and archiving - Terms and definitions";
8. Doctrine of information security;
9. Astakhova L.V. Theory of information security and methodology of information protection: methodical manual / L.V. Astakhov. - Chelyabinsk: Publishing House of SUSU, 2007. - 359 p.;
10. Yudin, E.G. Methodology of science. Consistency. Activities / E.G. Yudin. - M.: Editorial URSS, 1997. - 246 p.;
11. Borovsky A. S., Ryapolova E. I. Building a model of a protection system in cloud technologies based on a multi-agent approach using an automatic model