РАННЕЕ ПРЕДУПРЕЖДЕНИЕ при компьютерных атаках

Д.Костров, директор по информационной безопасности САП СНГ

УДК 004.056.53, DOI: 10.22184/2070-8963.2017.67.6.70.71

Подписанный Президентом РФ 26 июля 2017 года №187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" ускоряет необходимость создания системы раннего предупреждения при компьютерных атаках с учетом лучших практик, прогнозной аналитики и систем обработки Больших данных.

Согласно закону, к критической информационной инфраструктуре (КИИ) будут относиться информационные системы и информационно-телекоммуникационные сети госорганов, а также автоматизированные системы управления технологическими процессами в оборонной индустрии, в здравоохранении, связи, на транспорте, в кредитно-финансовой сфере, энергетике, а также в ряде отраслей промышленности (топливной, атомной, ракетно-космической, металлургической, химической, горнодобывающей). Кроме того, в перечень объектов КИИ включены организации в сфере науки.

У многих при словосочетании "система раннего предупреждения" возникает ассоциация с "ракетным нападением". Система предупреждения о ракетном нападении начала создаваться в середине 1950-х годов. Это специальная комплексная система для обнаружения запуска баллистических ракет, вычисления их траектории и передачи в командный центр противоракетной обороны информации, на основе которой фиксируется факт нападения на государство с применением ракетного оружия и принимается оперативное решение об ответных действиях. Такую систему необходимо создавать и в "виртуальном мире".

В мире уже действуют подобные центры, в России нам известны: центры мониторинга информационной безопасности системы распределенных ситуационных центров органов государственной власти РФ, государственные и корпоративные сегменты Системы обнаружения, предупреждения и ликвидации последствий компьютерных атак, система предупреждения и обнаружения компьютерных атак Министерства обороны РФ, система анализа трафика и обнаружения сетевых атак ПАО "Ростелеком" и т.п.

Необходимо отметить, что названные ситуационные центры способны детектировать и частично отражать уже осуществляющиеся атаки, но не в состоянии заблаговременно предупредить и пресечь атакующие воздействия. И это очень большая проблема. Поэтому на смену ранним принципам / концепциям построения центров реагирования на компьютерные атаки, построенных на основе технологий управления данными, позволяющими только обобщить и отразить в автоматизированном режиме информацию о случившихся инцидентах информационной безопасности с учетом заранее запланированного сценария, приходит новая концепция управления знаниями о текущем и предполагаемом информационном противодействии в киберпространстве. Это – возможность создавать когнитивные семантические информационно-аналитические системы и проводить автоматизированный контент-анализ в режиме реального времени.

В зарубежной практике такие технологии уже используются. Это программные решения Palantir, IBM, SAP, SAS и др. Основная концепция – визуализация Больших данных из разнородных источников, позволяющих находить взаимосвязи между объектами, обнаруживать совпадения между объектами и событиями вокруг них, выявлять аномальные объекты и т.п. Источниками информации выступают различные открытые и закрытые базы данных, структурированные и не структурированные источники информации, СМИ, социальные сети, мессенджеры.

Если рассматривать когнитивную систему раннего предупреждения о компьютерном нападении, то нужно выделить подсистемы, которые должны быть разработаны в обязательном порядке: сбора данных и знаний; предварительной обработки и анализа Больших данных; хранения данных и знаний; моделирования, подготовки и принятия решений; визуализации и администрирования.

Одним из основных является аналитический компонент с функциями: раннего предупреждения о компьютерном нападении на информационные ресурсы; выявления и порождения новых полезных знаний о качественных характеристиках и количественных закономерностях информационного противоборства; прогнозирования инцидентов безопасности, вызванных известными и ранее неизвестными компьютерными атаками; подготовки сценариев сдерживания противника в киберпространстве и планирования ответных действий, адекватных атаке и т.п.

При оценке возможности создания когнитивной системы раннего предупреждения необходимо отдавать себе отчет, что классическое понимание "импортозамещения" здесь не работает. Очень мало отечественных программных продуктов (не говоря уже об аппаратных) способны выполнить те требования, которые эта система должна обеспечивать. На помощь приходит сертификация иностранных программных продуктов по требованиям информационной безопасности от ФСТЭК России. Это проверка исходного кода на отсутствие недекларированных возможностей, создание и проверка продуктов с функциями безопасности по техническим условиям или СВТ.

В основе возможной архитектуры когнитивной системы должна лежать in-memory база данных, а требуемая семантика должна реализовываться на Master Data Management. Компонент системы "Сбор больших данных" должен создаваться на основе решений класса Extract\Transform\Leverage, которые осуществляют сбор данных из различных источников. При этом могут быть задействованы как типовые адаптеры (например, для Oracle, MS SQL, DB2, Hive), так и специализированные. Также должны быть развернуты решения типа Process Orchestration для интеграции с системами, поддерживающими механизмы очередей и обмена сообщениями. Обмен может проходить как в синхронном, так и в асинхронном режимах. Далее структурированные данные загружаются в хранилище данных, а не структурированные – в Extended Enterprise Content Management.

Компонент "Хранилище данных" создается на основе СУБД, которая может функционировать в оперативной памяти. СУБД in-memory преодолевает основной недостаток традиционных СУБД, состоящий в снижении производительности при обращении к дисковой памяти. Желательно, чтобы база данных использовала так называемый "поколоночный" тип хранения данных.

Компонент "Прогнозная аналитика" должен создаваться на основе так называемых решений BusinessObject BI Platform. Эти платформы поддерживают такие функции, как формирование отчетов произвольной сложности, выгрузка отчетов в различных форматах, автоматическая рассылка отчетов потребителям информации и проч. Система должна иметь возможность использовать встроенные библиотеки прогнозных алгоритмов (PAL), а при необходимости использования специфических математических методов они могут быть реализованы в специализированных библиотеках функций (AFL).

Применение когнитивных решений поможет перейти к так называемому семантическому управлению кибербезопасностью. Переход к применению семантических технологий при создании системы предупреждения является критически важной инновацией, которая определяет в среднесрочной перспективе основной вектор развития и источник технологических преимуществ создаваемых систем обнаружения, предупреждения и ликвидации последствий компьютерных атак на различные информационные ресурсы в нашей стране. ■