ОБ ИСПОЛЬЗОВАНИИ МЕТОДОВ ПРЕДИКТИВНОГО АНАЛИЗА ДЛЯ ЗАЩИТЫ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Миронова Наталия Генадьевна
кандидат филос.наук, доцент
ФГБОУ ВО Башкирский государственный университет
(Институт истории и государственного управления)
Уфа

АННОТАЦИЯ

Целью работы стал аналитический обзор интеллектуальных технологий и методов с предсказательным потенциалом для решения задач защиты информационной инфраструктуры, позволяющих создать более защищенную среду; обозначены некоторые «вторичные» проблемы для защиты, связанные с самой методологией реализации средств обеспечения безопасности, и возможные направлении их решения.

ABSTRACT

The aim of the work was an analytical review of intelligent technologies and methods with predictive potential for solving the problems of protecting information infrastructure, allowing you to create a more secure environment; some "secondary" problems for protection associated with the very methodology for the implementation of security measures are identified, and possible directions for solving.

Ключевые слова: информационная безопасность, предиктивная аналитика, поведенческий анализ, автоматизация защиты информации.

Keywords: information security, predictive analytics, behavioral analysis, UEBA, information security automation

Методы интеллектуального анализа данных используются для решения задач автоматизации процессов, в тех случаях, когда требуется высокая скорость принятия решений, а объем обрабатываемой информации в единицу времени превышает возможности человека-специалиста. К подобным задачам в настоящее время относится и обеспечение информационной безопасности информационной инфраструктуры предприятий, крупных организаций, ЦОД, сетевых ресурсов. Для некоторых категорий инфраструктуры количество инцидентов безопасности и атак может исчисляться сотнями тысяч за сутки, сложность атак постоянно нарастает, злоумышленники используют все более мощные инструменты автоматизации для проведения атак или несанкционированного доступа к защищаемым объектам. В этих обстоятельствах реактивная защита становится недостаточно эффективной и должна дополняться проактивной (в т.ч. автоматизированной), защитой, компенсирующей слабости «человеческого фактора».

Методы предиктивной/(предсказательной) аналитики, применяемые для задач обеспечения информационной безопасности различны. Для прогнозирования используются математические модели, методы интеллектуального анализа данных, машинного обучения. Суть общего подхода к прогнозированию в задачах обеспечения безопасности заключается в определении параметров, влияющих на прогнозируемое событие (угрозу безопасности, уязвимость), - или определение признаков, «маяков», косвенно указывающих на риск реализации угрозы ИБ с определенной вероятностью. Подход к прогнозированию рисков, заимствованный из области прогнозирования дефектов в работе промышленного оборудования (который состоит в обнаружении отклонений в работе оборудования от нормального состояния путем сравнения массивов данных, поступающих с датчиков в режиме реального времени, от штатной работы оборудования в нормальном режиме) – лишь частично пригоден для прогнозирования инцидентов безопасности, т.к. информационная инфраструктура как объект прогнозирования рисков ИБ менее статична, более сложна, чем промышленные АСУ как объект прогнозирования сбоев. Угрозы возникают не столько из-за технических поломок, сколько из-за целенаправленных и продуманных действий нарушителей, которые быстро адаптируются к существующим методам и инструментам защиты, постоянно ищут новые сценарии и способы воздействия, да и информационные технологии по мере развития и средства автоматизации, по мере их массированного внедрения, создают новые уязвимости. Пример – электронный документооборот, - который более уязвим к утечкам, тем традиционный документооборот именно потому, что он стал электронным.

Одно из направлений предиктивной аналитики в информационной безопасности – поведенческий анализ. Разработчики таких средств защиты, как системы обнаружения и предотвращения вторжений во внутреннюю сетевую инфраструктуру предприятия/компании начинают применять поведенческий анализ для автоматизации функции перехвата и реагирования на инциденты информационной безопасности. Потенциал методов поведенческой аналитики может применяться при решении задач противодействия разведке, для борьбы с мошенничеством (анти-фрод) и дискредитацией информации, для обнаружения признаков совершаемых атак, растянутых во времени

(подобные сложные задачи не решаются рутинным образом, пока не поддаются автоматизации в средствах защиты), для обнаружения неизвестных атак, для прогнозирования угроз и новых уязвимостей, возникающих в защищаемой системе в связи с появлением у злоумышленников новых технологических возможностей и сценариев атак и т.д. Для решения подобных задач предпринимаются усилия в направлении «интеллектуализации» систем защиты (в т.ч. совершенствования методов машинного обучения, развитии методологии оценки рисков ИБ, выявления корреляции событий безопасности).

Поведенческий анализ в области информационной безопасности – новая технология, реализуется, например, в формате систем анализа поведения пользователей и сущностей (User and Entity Behavior Analytics), которые представляют собой средства автоматизации обработки информации о разнообразных действиях пользователей и программных процессах; технология UEBA позволяет профилировать нормальное и аномальное поведение субъектов (людей, программных процессов, файлов), чтобы обнаружить несанкционированные действий в отношении объектов защиты. Поведенческий анализ в информационной безопасности позволяет выполнять классификацию событий безопасности, регистрировать инциденты, выявляя их источник и, в отдельных случаях, пресекать инцидент, в других случаях – предсказывать угрозы, уязвимостей, риски, векторы реализации угроз ИБ. Инструменты на основе методов поведенческого анализа позволяют анализировать работу почтовых сервисов, сетевую активность программ и людей в защищаемом информационном «периметре», регистрировать угрозы кражи, несанкционированного доступа к информации и объектам, попытки изменения настроек системы безопасности; прогнозировать поведение субъектов в защищаемой информационной системе системы с учетом собранных данных о более раннем их поведении и формируемых профилей и графов коммуникаций. Технология UEBA используется в системах управления и администрирования идентификации, в SIEM-системах, для формирования системы оценки рисков в компании/организаии. Технология UEBA может реализоваться на основе баз правил и исключений, сигнатур, методов статистического анализа, машинного обучения. Технологии машинного обучения (в т.ч. байесовы, иммунные, нейронные сети) все чаще находят применение для автоматизации решения задач ИБ. Например, генеративно-состязательные сети (GAN) используются для детектирования и выявления аномалий в сетевом трафике и поведении пользователей, для анализа клавиатурного почерка. Нейросетевые модели для автоматизации функций системы безопасности, дополняя возможности ИБ-специалиста, позволяют оперативно обрабатывать значительные массивы данных о событиях безопасности полнее и быстрее группы людей-специалистов, повышая общую эффективность, уровень оркестровки системы защиты. Конкретные области приложения нейросетевых методов, помимо систем поведенческого анализа, - сбор и корреляция данных о событиях ИБ в SOAR-системах; реагирование на инциденты информационной безопасности в IRP-системах; аутентификация и идентификация пользователей защищаемой системы посредством биометрических СКУД и иных системах распознавания; контроль сетевого трафика и реагирования на атаки (IDS/IPS, DLP-системы) и отсечение спама и части вредоносной активности со стороны внешних нарушителей; межсетевые экраны для сетевого прогнозного анализа (NGFW), которые находят применение для защиты от DDoS-атак и DNS-запросов, способны пресечь несанкционированный сбора информации программой-шпионом или изменение настроек, прерывать соединение с бот-сетями, проверять и блокировать почте фишинговые ссылки; выявление вредоносного кода (в антивирусах); реагирование на инциденты, их расследование, восстановление после сбоев; системы анализа сетевого трафика на основе машинного обучения; инструменты для автоматизации анализа уязвимостей. Поведенческий анализ может основываться, например, на анализе рабочих процессов или отдельных событий, сверяемых с неким регламентом, паттерном или цепочкой событий; отклонение от некой «нормы» считается признаком аномалии, требующим внимания и принятия решений о реагировании. Паттерном может быть «типичное» поведение нарушителя[1] или легального пользователя и т.п.

Модели поведенческого анализа не лишены ошибок первого и второго рода, т.е. событие может детектироваться системой обнаружения как угроза (угрозой не являясь) или, наоборот, аномальная активность может быть воспринята SIEM-системой как легитимная, не закрывая уязвимость. Одним из путей снижения уровня ошибок является расширение базы данных, возможность постоянно дообучать модель, а также пути увеличения прозрачности самого процесса принятия решения моделью (что позволяет проконтролировать корректность ее «логики»). Для увеличения прозрачности логики принятия решения об угрозе нейросетевыми инструментами и снижения числа

[1] Например, по оценке компании-разработчика средств защиты InfoWatch (см., например, сайт компании: https://www.infowatch.ru/products/prediction), типичным поведением (2/3 случаев) перед увольнением сотрудников является попытка скопировать корпоративные данные, чтобы использовать их в дальнейшем на новом месте. Подобное поведение может намекать на подготовку к увольнению и использоваться для прогнозирования угроз со стороны внутренних нарушителей в подобных обстоятельствах

ошибок перспективным могут быть модели интерпретируемого машинного обучения (interpretable machine learning); другое название подобных методов eXplainable Artificial Intelligence, XAI ([4], [5]). Существуют методы извлечения знаний из нейросетей: DeepLIFT ([6], [7]), PatternNet, алгоритм DeepRED для DNN, методы «релевантности признаков», визуального объяснения, автогенерация текстовых объяснений для CNN, методов релевантности признаков для RNN-сетей, а также сочетание нейросетевых моделей с другими методами (например, использование гибридных нейро-экспертных или нейро-нечетких систем), которые в будущем найдут, полагаем, более широкое применение и в инструментах информационной безопасности [1].

Хотя в UEBA-системах анализ поведения процессов и пользователей позволяет постоянно корректировать их профили, чтобы обнаруживать аномалии, но против отложенных сложных атак и угроз злоупотреблений со стороны инсайдеров и системы поведенческого анализа могут быть неэффективны. Если зарегистрированный пользователь в системе на протяжении долгого времени выполнял только легальные действия, в будущем его мотивы могут измениться (например, при угрозе увольнения или из-за подкупа со стороны внешних злоумышленников); каков в будущем окажется сценарий его вредоносных действий, сложно понять и формализовать, например, он может в будущем маскироваться под легальную активность, которая не распознается как аномалия. Еще разнообразнее риски реализации ранее неизвестных угроз со стороны ряда категорий потенциальных внешних нарушителей, о которых UEBA-система не имеет никаких сведений для анализа активности. Для решения задач этого класса для обеспечения безопасности информационной инфраструктуры, помимо средств на основе дескриптивной и диагностической аналитики, отдельным эшелоном защиты могут служить другие методы (и средства защиты) предиктивной аналитики.

Прогнозирование в ИБ реализуется на основе оптимизационных методов, статического анализа, нейросетевых моделей, эволюционных алгоритмов (например, [3]); для нейросетевых систем защиты информации эволюционные методы и генетические алгоритмы используют для минимизации ошибки обучения нейронной сети [2] и т.п.

Автоматизация анализа в сфере безопасности предполагает сбор, разметку, агрегацию разнообразных данных о ресурсах, событиях и пользователях защищаемой системы, - и надо понимать, что сама автоматизация процедур защиты и вспомогательных процессов повышает прозрачность защищаемой системы и, как следствие, рост разнообразия уязвимостей, связанных с использованием сырых и обработанных сведений на платформах обработки данных безопасности. Поэтому у автоматизации защиты есть и оборотная стороны, требующая дополнительного внимания и дополнительных усилий по защите. Тем не менее, новые методы и технологии обеспечения безопасности, помимо основной задачи защиты информационной инфраструктуры, могут дать общее технологическое усовершенствования рабочих и технологических процессов предприятий и компаний, усиливая их конкурентные позиций, поэтому руководителям следует анализировать тенденции в сфере технологий безопасности, чтобы понимать, в какие инновационные решения стоит вкладывать время и деньги и как они могут помочь общему развитию компании или предприятия.

Список литературы

Миронова Н.Г. Философское осмысление социальных рисков интеллектуальной автоматизации социального управления // Цифровой ученый: лаборатория философа. 2021. Т. 4. № 2. С. 125-144. DOI: 10.32326/2618-9267-2021-4-2-125-144 - URL: https://www.elibrary.ru/item.asp?id=47145602

Суханов А.В. Разработка теоретических основ и методологии мониторинга безопасности информационных систем для критических схем применениям // Диссертация на соискание ученой степени доктора технических наук, СПб, 2010, С. 368.

Учёные РФ применят генетические алгоритмы в системах цифровой безопасности предприятий // Информационный портал «Будущее России. Национальные проекты», Москва. [Дата публикации: 08.09.2020]

Arrieta A.B., Díaz-Rodríguez N., Del Ser J., Bennetot A., Tabik S., Barbado A., Garcia S., Gil-Lopez S., Molina D., Benjamins R., Chatila R., Herrera F. Explainable Artificial Intelligence (XAI): concepts, taxonomies, opportunities and challenges toward responsible AI // Information Fusion. Vol. 58. 2020. P. 82-115. URL: https://www.sciencedirect.com/science/article/pii/S1566253519308103 (дата обращения: 3.04.2021)

Knight W. DARPA is funding projects that will try to open up AI's black boxes // MIT Technology Review. 2017. URL: https://www.technologyreview.com/2017/04/13/152590/the-financial-world-wants-to-open-ais-black-boxes (дата обращения: 5.04.2021)

Shrikumar A., Greenside P., Kundaje A. Learning Important Features Through Propagating Activation Differences – URL: https://www.arxiv-vanity.com/papers/1704.02685;

Shrikumar A., Greenside P., Shcherbina A., Kundaje A. Not just a black box: Learning important features through propagating activation differences. arXiv preprint arXiv:1605.01713, 2016. – URL: https://www.arxiv-vanity.com/papers/1605.01713/