Научная статья
Original article
УДК 004.424

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ARTIFICIAL INTELLIGENCE IN INFORMATION SECURITY

Куренная Валерия Олеговна, студент бакалавр, Донской государственный технический университет, г. Ростов-на-Дону (344003 Россия г. Ростов-на-Дону, Гагарина 1), kurinaaa@rambler.ru

Kurennaya Valeria Olegovna, bachelor student, Don State Technical University, Rostov-on-Don (344003 Russia, Rostov-on-Don, Gagarina 1), kurinaaa@rambler.ru

Аннотация. Применение искусственного интеллекта неизбежно приведет к скачку в производстве, передаче и хранении информации и изменению ее характеристик. Информационная безопасность также будет иметь новые характеристики. Искусственный интеллект играет все более важную роль в области информационной безопасности, особенно в области обороны и нападения.

Abstract. The use of artificial intelligence will inevitably lead to a leap in the production, transmission and storage of information and a change in its characteristics. Information security will also have new characteristics. Artificial intelligence plays an increasingly important role in the field of information security, especially in the field of defense and attack.

Ключевые слова: информационная безопасность, искусственный интеллект.

Keywords: information security, artificial intelligence.

На сегодняшний день искусственный интеллект является актуальной информацией в Интернете и в категориях информационных навыков. Информационная безопасность, несомненно, является основой любых данных. Информационная безопасность требует соблюдения конфиденциальности, целостности и доступности информации, предотвращения несанкционированного раскрытия и использования информации, предотвращения фальсификации и уничтожения информации, а также обеспечения того, чтобы авторизованные пользователи и программы могли использовать информацию своевременно. Искусственный интеллект в информационной безопасности в приложении не имеет существенных изменений, но применение искусственного интеллекта приведет к скачку генерации и передачи информации и изменению характеристик, а также к новым возможностям информационной безопасности. Например, растущее число вирусов, таких как вирус WannaCry, вирус Petya и вирус CopyCat, привлекло к информационной безопасности беспрецедентное внимание. Искусственный интеллект играет все более важную роль в информационной безопасности, особенно в защите и нападении. Как правильно использовать и улучшить защиту за счет улучшения информационной безопасности стали горячей темой в отрасли.

Несколько стратегий искусственного интеллекта в мире коснулись информационной безопасности. Хотя подробные описания различны, общая логика в основном одинакова, включая следующие аспекты:

1) надежность, это основной показатель безопасности и контроля искусственного интеллекта. То есть работа видимым для пользователя способом; доверенный, то есть вывод системы, приемлемый для пользователя;

2) проверяемость и допустимость являются логически естественными расширениями двусмысленности и достоверности.

3) вопросы морали и конфиденциальности в первую очередь связаны с чувствительностью данных -слепой искусственный интеллектуальные алгоритмы для ошибок и неправильного использования, а также опасения по поводу возможных последствий пола, возраста, расы или экономической информации.

4) ответственность означает ответственность планировщиков и организаторов системы искусственного интеллекта в отношении результатов поведения системы искусственного интеллекта.

Сравнивая вышеперечисленные аспекты, проблема режима ответственности является более целенаправленной, и теперь она в основном отражается в разделении ответственности за несчастные случаи, например, во время вождения автомобиля.

Искусственный интеллект разрушает существующую индустрию информационной безопасности

Например, выявление утечек паролей и неправильное использование является хорошим примером. Этот тип атаки становится все более распространенным, поскольку электронные письма и пароли людей попадают в темные сети после утечки данных. Например, уязвимость Equifax привела к раскрытию миллионов действительных писем; в Yahoo! нарушение данных злоумышленники получили информацию об учетной записи на 500 миллионов 7-я ежегодная международная конференция по геопространственным знаниям и интеллекту.

Поскольку люди склонны повторно использовать пароли, преступники будут случайным образом пробовать разные электронные письма и пароли на разных машинах в надежде на успех. Чтобы идентифицировать этот тип атаки, искусственный интеллект устанавливает базовый уровень для пользователей, которые подключаются и входят в систему на нескольких устройствах каждый день. Для человека принято пробовать сотни логинов на сервере, но трудно найти человека, пытающегося подключиться на 100 разных машинах и войти только один раз. Искусственный интеллект также может использоваться для автоматической оценки потенциальных ошибок в открытом исходном коде.

Однако другим приложением с точки зрения уязвимости является обзор и прогнозирование. Если объявлена новая уязвимость, можно использовать данные журнала, чтобы узнать, использовалась ли она в прошлом. Или, если это действительно новая атака, искусственный интеллект может оценить, достаточно ли доказательств, чтобы определить, каков следующий шаг злоумышленника.

Искусственный интеллект также хорошо справляется с утомительными, повторяющимися задачами, такими как поиск определенного шаблона. Его реализация может облегчить ограничения ресурсов, с которыми сталкиваются большинство центров управления безопасностью.

Методы защиты привилегированных пользователей

Высокое значение учетной записи привилегированного пользователя. Привилегированные пользователи часто становятся жертвами атак Advanced Persistent Threat (APT). Цель состоит в том, чтобы заставить привилегированного пользователя раскрыть учетные данные или загрузить вредоносное ПО. Это дает злоумышленнику плацдарм в сети.

Злой умысел. Привилегированные пользователи могут преднамеренно подвергать опасности данные организации для личной выгоды, шпионажа или других злонамеренных целей. Они могут действовать как «волк-одиночка» или сотрудничать с хакерской группой или бизнес-конкурентом. Примеры злонамеренных намерений включают в себя:

Внедрение логической бомбы, троянского коня, бэкдора или вредоносного ПО в систему организации.

Развертывание вируса или вредоносного ПО в системах клиентов.

Сбор конфиденциальных или служебных данных.

Мониторинг привилегированных пользователей

Мониторинг привилегированных пользователей сопряжен со значительными техническими и операционными трудностями, поскольку привилегированным пользователям для выполнения своей работы требуется неограниченный доступ. Кроме того, технологические стратегии должны выходить за рамки встроенного аудита баз данных или управления информационными событиями безопасности (SIEM), поскольку эти инструменты предоставляют огромные объемы информации, но мало контекста, с помощью которого можно понять предупреждения.

Вместо этого надежная технологическая стратегия позволяет организации:

Отслеживание привилегированного доступа к конфиденциальным данным: отслеживайте доступ всех привилегированных пользователей к файлам и базам

данных (включая доступ к локальной системе), проверяйте создание пользователей и новые предоставленные привилегии и ограничивайте использование учетных записей с общими привилегиями.

Блокировать или предупреждать о подозрительных действиях: выявлять поведение пользователей, которое отличается от обычных шаблонов доступа, а также предупреждать и блокировать подозрительные действия, которые могут указывать на злоупотребление привилегиями. Пользователи, выполняющие несанкционированные действия, должны быть помещены в карантин, а их привилегии должны быть пересмотрены. Аудиторские отчеты и аналитические инструменты необходимы для поддержки судебных расследований.

Выявление несанкционированных изменений привилегий: убедитесь, что изменения в объектах данных и системах данных должным образом авторизованы. Несанкционированные действия должны быть тщательно расследованы, и должны быть реализованы меры контроля для предотвращения будущих инцидентов.

Разделение обязанностей: убедитесь, что привилегированные пользователи не могут контролировать себя, так как они могут изменять элементы управления безопасностью, чтобы скрыть свои нестандартные действия.

Устранение избыточных и неиспользуемых прав: определение пользователей с высокими привилегиями, проверка того, что привилегии необходимы для роли и обязанностей пользователя, отмена чрезмерных прав пользователя и удаление бездействующих пользователей.

Литература

1. Ван Хайтао Исследование системы осведомленности об информационной безопасности на основе технологий больших данных и искусственного интеллекта, Технологии и приложения сетевой безопасности, 2018 (3): 60-63.
2. Чжэн Яньфан Исследования и практика применения искусственного интеллекта и технологий анализа в системе ситуационной осведомленности информационной безопасности Мир цифровых коммуникаций, 2018, № 160 (4): 229.
3. Чжэн Фан Информационная безопасность в эпоху искусственного интеллекта, Исследования в области информационной безопасности, 2017, 3 (11): 966-967.

4. Дэн Вэньбинь Проблемы и меры противодействия надзору за информационной безопасностью в эпоху искусственного интеллекта Информационная безопасность Китая, 2018 г., 106 (10): 106-108.

References

1. Wang Haitao Research on Information Security Situation Awareness System Based on Big Data and Artificial Intelligence Technology, Network Security Technology and Application, 2018 (3): 60-63.
2. Zheng Yanfang Research and Practice of Artificial Intelligence Application and Analysis Technology in Information Security Situational Awareness System Digital Communication World, 2018, No.160 (4):229.
3. Zheng Fang Information Security in the Age of Artificial Intelligence, Information Security Research, 2017, 3 (11): 966-967.
4. Deng Wenbing Challenges and Countermeasures for Information Security Supervision in the Age of Artificial Intelligence China Information Security, 2018, 106 (10): 106-108.

© Куренная В.О., 2022 Научно-образовательный журнал для студентов и преподавателей «StudNet» №6/2022.

Для цитирования: Куренная В.О. ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ // Научно-образовательный журнал для студентов и преподавателей «StudNet» №6/2022.