Секция «HR в государственном управлении и администрировании: высококвалифицированные специалисты или искусственный интеллект - pro et contra»

Кибербезопасность и искусственный интеллект

Научный руководитель – Панич Наталья Александровна

Доу Вэй
Студент (магистр)
Московский государственный университет имени М.В.Ломоносова, Высшая школа государственного администрирования (факультет), Москва, Россия
E-mail: 2501820305@qq.com

Статистика показала, что что по мере роста цифрового бизнеса риск кибератак сильно возрастает. Проводилось исследование в Китае. 21% опрошенных заявили, что в 2018 году их организация столкнулась с нарушением кибербезопасности, что привело к несанкционированному доступу к информационным ресурсам.

Предприятия платят высокую цену за нарушения кибербезопасности: 20% сообщают о потерях в размере более 50 миллионов долларов. Последнее исследование Centrify показало, что https://www.centrify.com/resources/industry-research/pam-survey/ связаны с доступом к привилегированной учетной записи. То есть злоумышленники целенаправленно ищут учётные записи с максимумом прав, чтобы забрать ценную информацию из корпоративной системы и выгодно продать её.

Безусловно, крупный бизнес — самый лакомый кусок. Но ИТ-служба там обычно посильнее, а большинство уязвимых мест закрыты. Шансы добраться до чего-то ценного невелики. Совсем другая история со средними и небольшими компаниями. Компетентность штатных специалистов у них нередко оставляет желать лучшего. Как результат — не просто лазейки, а открытые двери для злоумышленников всех мастей. В чем же причина происходящего?

56% руководителей высшего звена признают, что их аналитики кибербезопасности перегружены и почти четверть (23%) не в состоянии успешно расследовать все выявленные инциденты. Capgemini обнаружил, что хакерские организации по-прежнему успешно используют алгоритмы отправки «фишинговых» сообщений целевым пользователям, для получения конфиденциальной информации.

То есть зачастую колоссальная по масштабу работа службы ИТ-безопасности идёт насмарку из-за банального человеческого любопытства и невнимания, а также чрезмерной нагрузки на сам отдел безопасности. Социальная инженерия эффективна, и чтобы помешать злоумышленникам, нужно попытаться пресечь получение подобных сообщений конечным пользователем. Искуственный интеллект вполне способен выступить в роли фильтра.

Преимущество искуственного интеллекта — в его способности работать быстрее человека и постоянно развиваться. В связи с введением GDPR и других нормативно-правовых актов, требующих защиты разных типов данных, необходимость в более надёжных системах защиты стала ещё более важной.

80% телекоммуникационных компаний говорят, что они рассчитывают на ИИ, способный выявлять угрозы и предотвращать кибератаки.

73% компаний тестируют варианты применения ИИ в сфере кибербезопасности, особое внимание уделяя вопросу безопасности конечных точек. Это важный момент, особенно если учесть, что по прогнозам количество конечных устройств (в том числе поддерживающих IoT) к 2021 году достигнет 24 млрд.

51% руководителей уже используют или работают над внедрением AI для раннего обнаружения киберугроз. Машинный разум способен значительно опережать традиционные системы прогнозирования и реагирования. Так что благодаря тому, что компании активно изучают вопрос внедрения и применения ИИ в рамках комплекса мер по обеспечению кибербезопасности, качество прогнозирования и скорость реагирования будут расти.

Почти две трети руководителей признают, что искуственный интеллект снижает затраты на выявление и реагирование на угрозы (экономия от 1% до 15%, в среднем 12%). Благодаря искуственному интеллекту общее время, необходимое для обнаружения угроз и нарушений, сокращается до 12%. А время задержки (количество времени, в течение которого злоумышленник остаётся незамеченным), уменьшается на 11%. Сокращение времени достигается за счёт постоянного сканирования известных или неизвестных аномалий, которые показывают паттерны угроз.

Этому есть реальные подтверждения. https://www.zdnet.com/article/how-technology-is-saving-petsmart-millions-by-eliminating-sales-fraud/, популярный магазин товаров для домашних животных в США, сэкономил $12 млн, используя AI для обнаружения мошенничества. В партнерстве с Kount PetSmart внедрил технологию AI/Deep Learning, которая изучает миллионы транзакций и их результаты. Умная система определяет легитимность каждой транзакции, сравнивая ее со всеми другими полученными транзакциями. Выявляемые мошеннические заказы отменяются, что позволяет экономить деньги компании, не нанося ущерба бренду.

Обнаружение мошенничества, обнаружение вредоносных программ, обнаружение вторжений, оценка риска в сети и анализ поведения пользователя — это пятёрка самых актуальных способов применения искуственного интеллекта для улучшения кибербезопасности.

Искуственный интеллект реально меняет привычные аспекты кибербезопасности. Он улучшает способности компаний предвидеть и предотвращать киберпреступления, защищает устройства с нулевым уровнем доверия, может контролировать даже устаревание паролей! То есть искусственный интеллект действительно необходим для обеспечения безопасности периметров любого бизнеса.

Поиск взаимосвязей между угрозами и анализ вредоносных файлов, подозрительных IP-адресов или необычную деятельность сотрудника длится считанные секунды или минуты То есть уже сейчас ИИ помогает человеку обеспечивать кибербезопасность. А в дальнейшем его возможности будут только расширяться, делая участие человека в процессе защиты чисто номинальным.

Взять те же банки — благодаря AI антифрод-системы станут работать надёжнее и быстрее, что позволит сэкономить нервы и деньги как клиентов финансовых учреждений, так и самих банкиров. А по мнению компании Dell, занимающейся разработкой в том числе и подобных продуктов, искуственный интеллект способен защитить, контролировать и отслеживать данные в гибридных средах, а также предотвращать 99% атак вредоносного ПО.