УДК 004.891.2

СИСТЕМА АНАЛИЗА ПОВЕДЕНИЯ ПОЛЬЗОВАТЕЛЕЙ ДЛЯ ВЫЯВЛЕНИЯ ВНУТРЕННИХ УГРОЗ

Боязитов И.Э. (Федеральное государственное бюджетное образовательное учреждение высшего образования «МИРЭА — Российский технологический университет»)
Научный руководитель – старший преподаватель Серебряков И.Е.
(Федеральное государственное бюджетное образовательное учреждение высшего образования «МИРЭА — Российский технологический университет»)

Аннотация.
В данной работе представлена система анализа поведения пользователей, которая позволяет выявлять угрозы внутри компании и уведомлять об этом администратора безопасности. Для обнаружения таких ранее неизвестных атак данная система использует нейронные сети.

Введение.

В настоящее время существует множество техник по предотвращению угроз информационной безопасности, однако они в основном направлены на внешние атаки. Угрозы, исходящие извне, предотвращаются системами обнаружения вторжений (СОВ), межсетевыми экранами (МЭ) и другими системами безопасности. В то время как внутренним нарушителям гораздо легче совершить злонамеренные действия и нанести гораздо больший ущерб, поскольку они находятся внутри компании и намного ближе к конфиденциальным данным. К таким нарушителям относятся: небрежные сотрудники, которые не соблюдают правила безопасной обработки данных; скомпрометированные сотрудники, личные данные которых утекли к злоумышленнику; злонамеренные сотрудники, которые могут попытаться отомстить компании после наказания или увольнения. Множество программных продуктов по информационной безопасности могут не выявить подобные угрозы, поскольку они смотрят на мир с бинарной точки зрения: трафик может быть плохим или хорошим, файлы заражены или не заражены, пользователи авторизованы или заблокированы. Во многих ситуациях эти подходы работают, но такое разделение на «черное и белое» имеет свои недостатки. Проникнув внутрь системы, новые типы целевых атак могут использоваться для неспешного наблюдения, исследования и эксплуатирования организации, обходя все традиционные средства защиты. Поэтому необходимо иметь дело и с «серой» частью – обнаружением таких слабых и медленных угроз. Для решения этой проблемы лучше всего подходит машинное обучение, которое обеспечивает выявление аномалий в действиях пользователей.

Основная часть.

Для выявления угроз внутренних нарушителей предлагается система анализа поведения пользователей, в основе которой используется один из видов машинного обучения – обучение без учителя. Система наблюдает за поведением каждого пользователя в сети для создания базовых моделей, характеризующих нормальное поведение. Для создания достаточно правильной модели требуется примерно 30 дней исторических данных. В качестве источников данных могут использоваться журналы авторизации, журналы передаваемого трафика в сети, журналы печати. Последующие действия пользователей оцениваются по их базовым моделям. При появлении отклонений от нормального поведения, пользователю назначается оценка от 0 до 100, в зависимости от критичности угрозы. Данное решение дополняет традиционные подходы, основанные на предопределенных правилах и сигнатурах, выявляя ранее неизвестные атаки и снижая количество ложных срабатываний.

Выводы.

В результате данной работы была представлена система анализа поведения пользователей. Данная система позволит повысить эффективность защиты от утечки конфиденциальных данных компании, что в конечном итоге позволит минимизировать репутационные риски и риски экономических потерь, что особенно важно в сегодняшних условиях высокой турбулентности макроэкономической среды.

Боязитов И.Э. (автор) Подпись

Серебряков И.Е. (научный руководитель) Подпись