Столыпинский
вестник

Научная статья
Original article
УДК 004.424

СТАНДАРТЫ КЛАССИФИКАЦИИ ДАННЫХ

DATA CLASSIFICATION STANDARDS

Крыгин Никита Дмитриевич, студент бакалавр, Донской государственный технический университет, г. Ростов-на-Дону (344003 Россия г. Ростов-на-Дону, Гагарина 1), krigginnn@rambler.ru

Krygin Nikita Dmitrievich, bachelor student, Don State Technical University, Rostov-on-Don (344003 Russia, Rostov-on-Don, Gagarina 1), krigginnn@rambler.ru

Аннотация: Цель и задача стандарта классификации данных — предоставить последовательное определение того, как организация должна обрабатывать и защищать различные типы данных. Элементы управления безопасностью защищают различные типы данных. Эти элементы управления безопасностью находятся в пределах семи доменов типичной ИТ-инфраструктуры. Процедуры и рекомендации должны определять, как обращаться с данными в семи доменах типичной ИТ-инфраструктуры для обеспечения безопасности данных.

Abstract: The purpose and purpose of a data classification standard is to provide a consistent definition of how an organization should process and protect different types of data. Security controls protect various types of data. These security controls fall within the seven domains of a typical -IT infrastructure. Procedures and guidelines

should define how data is handled in the seven domains of a typical IT infrastructure to ensure data security.

Ключевые слова: информационная безопасность, классификация данных, стандарт.

Keywords: information security, data classification, standard

Для предприятий и организаций, в соответствии с последними законами о соответствии, стандарты классификации данных обычно включают следующие основные категории:

Личные данные — данные о людях, которые должны храниться в тайне. Организации должны использовать надлежащие меры безопасности, чтобы соответствовать требованиям.

Конфиденциально — информация или данные, принадлежащие организации. Интеллектуальная собственность, списки клиентов, информация о ценах и патентах являются примерами конфиденциальных данных.

Только для внутреннего использования — информация или данные, используемые внутри организации. Хотя конфиденциальная информация или данные могут не включаться, сообщения не предназначены для выхода за пределы организации. Общественным достоянием — информация или данные, предоставляемые общественности, такие как содержимое веб-сайта, официальные документы и т. п

В зависимости от стандарта классификации данных вашей организации может потребоваться шифрование данных с наивысшей степенью конфиденциальности даже на устройствах хранения и жестких дисках. Например, вам может понадобиться использовать шифрование и технологию VPN при использовании общедоступного Интернета для удаленного доступа. Но внутренняя связь по локальной сети и доступ к системам, приложениям или данным могут не требовать использования шифрования.

Пользователям также может быть ограничен доступ к личным данным клиентов, и они могут иметь доступ только к определенным частям данных.

Представители службы поддержки клиентов обеспечивают обслуживание клиентов , не получая доступа ко всем личным данным клиентов. Например, они могут не видеть весь номер социального страхования или номера счетов клиента; могут быть видны только последние четыре цифры. Этот метод сокрытия некоторых символов чувствительного элемента данных называется маскированием.

Организации должны начать определение своей политики безопасности ИТ с определения политики классификации активов. Эта политика, в свою очередь, напрямую согласуется со стандартом классификации данных. Этот стандарт определяет способ, которым организация должна защищать свои данные. Исходя из вашего стандарта классификации данных, вам необходимо оценить, перемещаются ли какие-либо частные или конфиденциальные данные в любой из семи доменов типичной ИТ-инфраструктуры. В зависимости от того, как вы классифицируете и используете данные, вам потребуется применять соответствующие меры безопасности во всей ИТ-инфраструктуре.

Уровень спам-трафика электронной почты, поступающего через простой протокол передачи почты (SMTP) [6], около 90 % до или 50 % после IP-фильтрации, делает его фактически нефункциональным без фильтрации ни для пользователей, ни с экономической точки зрения.

Для компаний интернет-провайдеров. Большинство практических решений по борьбе со спамом основаны на краудсорсинге и частично на экспертном анализе. Учетных записей-приманок, привлекающих спам, для извлечения подписей из спама пример сообщения. Такие подписи включают IP-адреса, рукопожатие и источник.

Домены, домены заголовков, темы и другие текстовые заголовки, основной текст, URL-адреса и вложения. Фильтрация таких сигнатур обычно эффективна с точки зрения точности и скорость против несложного спама, составляющего около 90% всего спама. Однако такие сигнатуры становятся доступными только через несколько часов после начинается спам-атака с неизвестными ранее сигнатурами. А также ведение и поиск в базах данных сигнатур спама требует

либо значительных вычислений, либо ресурсы хранения на месте или платная подписка на провайдеров фильтрации спама.

Умные спамеры знают об этих ограничениях и используют их, проводя распределенные, кратковременные, интенсивные кампании. Алгоритмы глубокого обучения (DL) могут определять тональность и семантику интеллектуальный спам полнотекстовыми текстами [10, 4].

Однако алгоритмы глубокого обучения требуют значительно больше ресурсов и имеют более длительный срок службы время обработки по сравнению с более простыми алгоритмами. Хотя стандарты SMTP допускают множество время доставки сообщения получателю, современная электронная почта пользователи ожидают доставки сообщений почти в реальном времени. Поэтому медленный и дорогой DL алгоритмы, как правило, используются на последней линии защиты для сообщений с непонятный приговор. Еще одно косвенное влияние сканирования всего тела сообщения имеет теоретико-игровые последствия — оно увеличивает размер входящих спам-сообщений до максимальные ограничения, потому что спамеры пытаются перегрузить спам-фильтры. Следовательно, для этого используя анализ всего тела, интернет-провайдер должен быть готов к ресурсам для обработки меняющаяся структура и объем трафика.

Алгоритмы, основанные на поведении, используют упрощенную близость пространства признаков, анализ строки темы и других коротких текстовых заголовков, чтобы заполнить очевидный пробел между алгоритмами на основе статической подписи и семантикой всего тела DL.

Алгоритмы анализа настроений. Алгоритмы Bag of Words — популярный выбор для такого анализа [9]. Они используют от нескольких сотен до нескольких тысяч измерений пространства частотных словарей и различных границ расстояний и классов алгоритмы, такие как косинусные и евклидовы расстояния или машины опорных векторов (SVM) и алгоритмы регрессии искусственных нейронных сетей (ANN).

Однако, для моделей Bag of Words требуется предварительная обработка

текста и инфраструктура базы данных, которые потребляют время и аппаратные ресурсы.

Представленный алгоритм Bag of Synthetic Syllables (BoSS) является автономным, имеет простую логику быстрых вычислений, не требует никаких внешних ресурсов и вводит минимальные накладные расходы ЦП или памяти. Алгоритм BoSS можно рассматривать как связанный с алгоритмами n-граф с пользовательскими смеси из 2 и 1, который создает достаточно многомерного пространства для обработки коротких текстов, по-прежнему сохраняя низкие требования к обработке для поиска морфологических или стохастических вариационные окрестности [1, 9].

Литература

1. Алеексеев, П. Антивирусы. Настраиваем защиту компьютера от вирусов / П. Алеексеев, Д. Козлов, Р. Прокди. - М.: СПб: Наука и Техника, 2018. - 915 с.
2. Александров, К.П. Компьютер без сбоев, вирусов и проблем / К.П. Александров, Р.Г. Прокди. - М.: Наука и техника, 2017. - 192 с.
3. Алямовский, А.А. SolidWorks 2007/2008. Компьютерное моделирование в инженерной практике / А.А. Алямовский. - М.: СПб: БХВ-Петербург, 2017. - 845 с.
4. Большаков, В.П. Инженерная и компьютерная графика. Практикум: моногр. / В.П. Большаков. - М.: СПб: БХВ, 2020. - 592 с.
5. Бухбергер, Б. Компьютерная алгебра: символьные и алгебраические вычисления / Б. Бухбергер, Дж. Коллинз, Р. Лоос. - М.: [не указано], 2020. - 344 с.
6. Вульф, М.М. Защита компьютера от вирусов (книга + видеокурс на DVD) / М.М. Вульф, Н.Т. Разумовский. - М.: СПб: Наука и Техника, 2020. - 160 с.
7. Глушаков, С.В. Компьютерная верстка. QuarkXPress 4.1. Adobe PageMaker 6.52. Учебный курс / С.В. Глушаков, Г.А. Кнабе. - М.: Харьков: Фолио, 2016. - 485 с.
8. Глушаков, С.В. Компьютерная графика / С.В. Глушаков, Г.А. Кнабе. - М.: Харьков: Фолио, 2016. - 500 с.

9. Гурский, Ю. Компьютерная графика: Photoshop CS, CorelDRAW 12, Illustrator CS / Ю. Гурский, И. Гурская, А. Жвалевский. - М.: СПб: Питер, 2016. - 812 с.
10. Дабижа Компьютерная графика и верстка. CorelDRAW, Photoshop, PageMaker / Дабижа, Галина. - М.: СПб: Питер, 2017. - 272 с.
11. Девянин, П.Н. Анализ безопасности управления доступом и информационными потоками в компьютерных системах / П.Н. Девянин. - М.: Радио и связь, 2020. - 176 с.
12. Зарецкий, А.В. А я был в компьютерном городе / А.В. Зарецкий, А.В. Труханов. - М.: Просвещение, 2018. - 208 с.
13. Зенкин, А.А. Когнитивная компьютерная графика / А.А. Зенкин. - М.: Наука, 2018. - 192 с.
14. Касихин, В.В. Как стать создателем компьютерных игр. Краткое руководство / В.В. Касихин. - М.: Вильямс, 2016. - 208 с.
15. Кротов, Н.Н. Nero Burning ROM 8. Компьютерная шпаргалка / Н.Н. Кротов, Р.Г. Прогди. - М.: СПб: Наука и Техника, 2020. - 594 с.
16. Кук, Д. Компьютерная математика / Д. Кук, Г. Бейз. - М.: [не указано], 2020. - 431 с.

References

1. Alekseev, P. Antiviruses. Setting up computer protection against viruses / P. Alekseev, D. Kozlov, R. Prokdi. - M.: St. Petersburg: Science and Technology, 2018. - 915 p.
2. Alexandrov, K.P. Computer without failures, viruses and problems / K.P. Aleksandrov, R.G. Prokdi. - M.: Science and technology, 2017. - 192 p.
3. Alyamovsky, A.A. SolidWorks 2007/2008. Computer modeling in engineering practice / A.A. Alyamovsky. - M.: St. Petersburg: BHV-Petersburg, 2017. - 845 p.
4. Bolshakov, V.P. Engineering and computer graphics. Workshop: monograph. / V.P. Bolshakov. - M.: St. Petersburg: BHV, 2020. - 592 p.
5. Buchberger, B. Computer algebra: symbolic and algebraic calculations / B. Buchberger, J. Collins, R. Loos. - M.: [not specified], 2020. - 344 p.
6. Wolf, M.M. Protecting your computer from viruses (book + video course on DVD)

/ M.M. Wolf, N.T. Razumovsky. - M.: St. Petersburg: Science and Technology, 2020. - 160 p.

7. Glushakov, S.V. Computer layout. QuarkXPress 4.1. Adobe Page Maker 6.52. Training course / S.V. Glushakov, G.A. Knabe. - M.: Kharkov: Folio, 2016. - 485 p.
8. Glushakov, S.V. Computer graphics / S.V. Glushakov, G.A. Knabe. - M.: Kharkov: Folio, 2016. - 500 p.
9. Gursky, Yu. Computer graphics: Photoshop CS, CorelDRAW 12, Illustrator CS / Yu. Gursky, I. Gurskaya, A. Zhvalevsky. - M.: St. Petersburg: Piter, 2016. - 812 p.
10. Dabija Computer graphics and layout. CorelDRAW, Photoshop, PageMaker / Dabizha, Galina. - M.: St. Petersburg: Piter, 2017. - 272 p.
11. Devyanin, P.N. Security analysis of access control and information flows in computer systems / P.N. Devyanin. - M.: Radio and communication, 2020. - 176 p.
12. Zaretsky, A.V. And I was in a computer city / A.V. Zaretsky, A.V. Trukhanov. - M.: Education, 2018. - 208 p.
13. Zenkin, A.A. Cognitive computer graphics / A.A. Zenkin. - M.: Nauka, 2018. - 192 p.
14. Kasikhin, V.V. How to become a computer game creator. Brief guide / V.V. Kasikhin. - M.: Williams, 2016. - 208 p.
15. Krotov, N.N. Nero Burning ROM 8. Computer cheat sheet / N.N. Krotov, R.G. Progdie. - M.: St. Petersburg: Science and Technology, 2020. - 594 p.
16. Cook, D. Computer Mathematics / D. Cook, G. Baze. - M.: [not specified], 2020. - 431 p.

Для цитирования: Крыгин Н.Д. Стандарты классификации данных Научный сетевой журнал «Столыпинский вестник», номер 4/2022.