Тип работы: Дипломная работа

Предмет: Информационные системы и процессы

Оглавление

Введение
В настоящий момент времени наблюдают резкое количество инцидентов в области информационной безопасности, которые приобрели широкое распространение и имеют угрожающий характер для всех сфер жизни общества. Очень часто угрозы информационной безопасности называют атакам. В данном случае также следует придерживаться общепринятой терминологии. Большинство подобных атак имеют отношение к широкому кругу частных, корпоративных, а также государственных областей. Главные тенденции развития таких угроз состоят в следующем:
Увеличение количества атак, многие из которых обуславливают большие потери;
Нарастание сложности атаки, которая может иметь несколько этапов и использование специальных методов защиты от возможных методов вторжения;
Применимость атак практически ко всем электронным (цифровым) устройствам, в числе которых в последнее время все большое число относится к мобильным устройствам, а они в наибольшей степени могут подвергаться риску в области информационной безопасности;
Имеется все больше случаев нападения на информационные инфраструктуры крупных корпораций, важных промышленных объектов, а также государственных структур;
Использование наиболее прогрессивными в области компьютерной технологии странами средств и методов кибернападений на другие государства.
Актуальность темы исследования подтверждается практически ежедневными сообщениями, которые предоставляют данные о все новых атаках злоумышленников в информационной сфере. Число вредоносных объектов, которые обнаруживают в глобальной сети каждый год, исчисляют девятизначной цифрой, их распространение ведут с использование более чем 100 миллионов интернет-адресов [1], [2]. Каждый год количество вредоносных объектов возрастает на 40% [3]. Атаки в информационном пространстве наносят значительный ущерб, который оценивают более чем в 100 миллиардов долларов [4]. Данные тенденции обуславливают важность темы исследования «Защита информационной безопасности корпоративных Web-ресурсов».
Объектом данной работы является противодействие киберугрозам в сфере безопасности государственных и частных организаций.
Предмет работы – оценка рисков информационной безопасности с применением нейронных сетей. Цель работы состоит в рассмотрении использования нейронных сетей для оценки угроз информационной безопасности.
Для достижения цели работы необходимо выполнить следующие задачи:
1. Изучить базу OWASP и выявить наиболее актуальные угрозы безопасности.

2. Сравнить сканеры уязвимостей.
3. Описать объект защиты (поднятый веб-сервер или веб-сервер реальной организации).
4. Просканировать объект защиты на наличие уязвимостей.
5. Предложить мероприятия по устранению уязвимостей.
6. Сделать выводы

1. Аналитическая часть

1.1 Актуальные угрозы безопасности.

Управление рисками – процесс, включающий анализ рисков, выбор, реализация и оценка эффективных и экономичных контрмер, проверка, что риски установлены на приемлемом уровне. Управление рисками должно учитываться на каждом из этапов жизненного цикла ИС. На основе процесса управления рисками строится вся система информационной безопасности. Иногда для управления рисками применяют так называемый цикл pdca. Цикл Шухарта - Деминга (Цикл PDCA) – известная модель непрерывного улучшения процессов, получившая название цикла Шухарта - Деминга или цикла PDCA - планируй (Plan), делай (Do), проверяй (Check), воздействуй (Act), при ее применении в самых различных областях деятельности позволяет эффективно управлять этой деятельностью на системной основе. Основные задачи компонентов цикла: Оценка информационной безопасности является основополагающим этапом процесса управления рисками

Планирование - идентификация и анализ проблемы; оценка возможностей и планирование необходимых изменений.

Выполнение - поиск решения проблемы и осуществление запланированных мероприятий.

Проверка - оценка результатов и выводы в соответствии с поставленной задачей.

Действия - принятие решения на основе полученных выводов; если изменение не решает поставленную задачу следует повторить цикл, внеся коррективы в план.

Управление рисками – процесс, включающий анализ рисков, выбор, реализация и оценка эффективных и экономичных контрмер, проверка, что риски установлены на приемлемом уровне.

Управление рисками должно учитываться на каждом из этапов жизненного цикла ИС.

Однако многие традиционные методы анализа рисков безопасности становятся все более и более несостоятельными с точки зрения удобства использования, гибкости и критически недостаточными с точки зрения того, что они создают для пользователя [1].

Изучение основных элементов риска и внедрения методологии и инструментария оценки рисков безопасности в настоящее время используется многими крупнейшими мировыми корпорациями. Это изучение также включает использование одного и того же продукта для обеспечения соблюдения политики безопасности, внешних стандартов (таких как ISO 17799) и законодательства (например, законодательства о защите данных).

Рисунок 1. Процесс оценки рисков информационной безопасности

Безопасность в любой системе должна быть соизмерима с ее рисками. Тем не менее, процесс определения того, какие средства контроля безопасности являются приемлемыми и экономически эффективными, нередко является сложным, а иногда и субъективным. Одной из основных функций анализа риска безопасности является то, чтобы этот процесс был более объективным.

Существует ряд различных подходов к анализу рисков. Однако они, по существу, разбиваются на два типа: количественные и качественные.

Рисунок 2. Процесс управления риском ИБ

Количественный анализ рисков

В этом подходе используются два фундаментальных элемента; вероятность возникновения события и вероятные потери в случае его возникновения [12].

Количественный анализ рисков использует количественные параметры, полученные из этих элементов. Например, EF (exposure factor), AV – стоимость актива, SLE ожидаемые однократные потери (SLE=EF*AV), ARO-среднегодовая частота реализации. ALE – ожидаемые среднегодовые потери = SLE*ARO. Таким образом, теоретически можно оценивать события в порядке риска и принимать решения на основе этого. Проблемы с данным типом анализа рисков обычно связаны с ненадежностью и неточностью данных. Вероятность редко бывает точно определена и может в некоторых случаях способствовать ошибочности принятия решения. Кроме того, мероприятия контроля и контрмеры часто затрагивают ряд потенциальных событий, и сами события часто являются взаимосвязанными.

Несмотря на указанные недостатки, в ряде организаций успешно применяется количественный анализ рисков.
Качественный анализ рисков является, безусловно, наиболее широко используемым подходом к анализу рисков. Данные о вероятности событий не требуются и используют только оценочные потенциальные потери.
В большинстве качественных методологий анализа рисков используются некоторые взаимосвязанные элементы:
Пример качественной оценки рисков представлен в таблице 1.
Таблица 1. Пример качественной оценки рисков
Группы уязвимости
Содержание уязвимостей Активные счета Пассивные счета Страт. планы Инф. данные
1. Среда и инфраструктуры
Неправильное применение физических средств управления доступа в
здания низкий низкий низкий низкий
Нестабильная работа электросети низкий низкий низкий низкий
3. Программное обеспечение
Отсутствие механизма идентификации и аутентификации низкий низкий низкий низкий
Отсутствие аудиторских проверок низкий низкий низкий низкий
Неконтролируемая загрузка и применение программного обеспечения низкий низкий низкий низкий
4. Коммуникация
Незащищенность линий связи высокая высокий высокий высокий
Отсутствие идентификации и аутентификации отправителя и получателя высокий высокий высокий высокий
Отсутствие подтверждения посылок или получений сообщений высокий средний средний средний
5. Документ (документооборот)
Хранение в незащищенном месте низкий низкий низкий низкий
Бесконтрольное копирование низкий низкий низкий низкий
6.Персонал
Недостаточная подготовка персонала по вопросу обеспечения безопасности низкий низкий низкий низкий
Отсутствие механизма отслеживания низкий низкий низкий низкий

Угрозы.
Угроза - это событие, что что-то может пойти не так, или что-то можно «атаковать» систему. Примеры могут включать в себя пожар или мошенничество. Угрозы всегда присутствуют для каждой системы.
Уязвимости системы.
Слабые места делают систему более подверженной угрозам атаки или делают атаку более вероятной, чтобы она имела некоторый успех или действие. Для информационной системы банка уязвимость будет заключаться в наличие человеческого фактора при сохранении ценной информации (например, при хранении финансовых документов).
Контроль за процессами системы [9].
В литературных источниках чаще всего описываются четыре стратегии работы с рисками. Эти действия - принять риски, отказ от рисков, передача рисков, уменьшение рисков.
Стратегия уклонения предполагает полное исключение риска из проекта. Необходимо придумать реагирование, которое позволит быть уверенными, что риск не материализуется. Это самая «дорогая» стратегия, т.к. для некоторых рисков она вынуждает отказываться от определенных работ, менять цели проекта или, в самом радикальном случае, отказываться от проекта.
Стратегия передачи перекладывает последствия материализации риска и ответственность за реагирование на третью сторону, при этом сам риск не устраняется. Эта стратегия практически всегда предполагает финансовые затраты на передачу и получение финансовой компенсации в случае материализации риска.
Принятие риска - юридически значимое деяние (действие или бездействие) субъекта права, осуществленное применительно к рисковой ситуации и выраженное в избрании и реализации определенной стратегии управления рисками.
Стратегия уменьшения является самой распространенной и может применяться к любому риску, т.к. подразумевает уменьшение вероятности или влияния риска на проект. Опишем её подробнее.

Контролирование процессов в системе является контрмерой при наличии уязвимостей. Существует четыре типа осуществления контроля:
Сдерживающие средства контроля уменьшают вероятность преднамеренной атаки;
Профилактический контрольные мероприятия защищают уязвимости и делают атаку неудачной или уменьшает ее воздействие;
Корректирующие элементы контроля уменьшают эффект атак;
Детективные элементы контроля обнаруживают атаки и запускают профилактические или корректирующие элементы управления.
Эти элементы можно проиллюстрировать простой реляционной моделью:

Рисунок 3 Схема организации атак

1.2 Сравнение сканеров уязвимостей.
В настоящее время применяется большое количество методик для анализа риска. Некоторые из них имеют в основе достаточно простые табличные методы, и при их внедрении не предполагается использовать специализированное программное обеспечение. Другие средства анализа, напротив, активно используют специализированный программный инструментарий. Несмотря на возрастающий интерес к управлению риском в организациях, применяемые в настоящий момент времени методы являются достаточно неэффективными, так как эти процессы во многих фирмах осуществляются в каждом подразделении независимым образом. Организация централизованного контроля над этими мероприятиями зачастую не применяется, что приводит к исключению возможности реализации единых и целостных подходов к управлению риском во всей структуре организации.
Для решения задач оценки риска в области информационной безопасности в текущий момент времени наиболее часто применяют такие программные средства: CRAiMM, RiskWatch, FRAP, Microsoft Security Assessiment Tool (MSiAT), CORAS, ГРИФ и многие другие. Все известные методы могут быть разделены на:
- методы, которые используют оценку рисков на качественных уровнях (например, по ранжированной шкале «низкий уровень», «средний», «высокий уровень»), к таким методам, например, относят методику FRAP;
- методы, которые используют количественную методику (риски оценивают через числовые значения, например, величина ожидаемой годовой потери), к этому классу относят методику RiskWatch;
- методы, которые пользуются смешанными оценками (такие подходы используют в системе CRAMM или методике MSAT).
Еще до принятия окончательных решений о внедрении тех или иных методик управления риском информационной безопасности следует убедиться, что они достаточно полным образом учитывают бизнес-процессы организации, масштаб угроз, а также соответствуют общепринятой мировой практике и обладают достаточно подробным описанием процессов и необходимых мероприятий [3].
В таблице 2 представим результаты сравнительного анализа наиболее часто используемых в настоящее время методов (ГРИФ, CRAMM, RiskWatch, MSAT, CORAS).
Таблица 1 Сравнение программных комплексов для управления риском в области информационной безопасности.

Список использованных источников
1. Баранов А.К., Бабашов А.В. Безопасность информации и защита данных. – М.: ИНФР-М_РИР, 2014.
2. Баранов А.К. Методика и программное обеспечение для оценки риска в сфере безопасности информации // Управление рисками. 2014. № 1(49). С. 15–26.
3. Петренков А.А. Управление информационным риском. Экономически оправданные методы обеспечения безопасности / Петренков А.А., Симонова П.В. М.: Компания АТи; ДМ Пресс, 2014.
4. Международные стандарты ISO/IEC 2705:2017. Информационные технологии –Методы защиты безопасности информации – Менеджмент риска для информационной безопасности BS IS/IC 27005:2014.
5. Левченкова Р.Н. Стадии анализа риска. URL: http://www.cfn.ru/finanalysis/risks/ stages.shtml
6. Requirement and Models for IDE - A Real-Time Intrusions-Detection Expert Systems, Final Reports, Dorothy Dennin and Peter G. Nemann, Computer Science Laboratory, SRIS Internationals, August 2015.
7. A Prototype IDE: A Real-Times Intrusion-Detections Expert Systems, Final Reports, Dorothy E. DENNINGs, David E. Edward, R. Jagamathans, Teresa F. Lunter and Peter G. Neumanns, Computer Sciences Laboratories, August 2017.
8. IDES: The Enhaced Prototypes, A Real-Time Intrusions Detection Experts Systems, Teresa F. Lunter, R.

Jagannathaner, Rosatmas Lee, Sherryl Lstgarten, David L. Edwarder, Peter G. Neumanns, Harold S. Javitzer and Al Valde, SRI-CSL-8-12, SRI Project 485-01, October 2008.
9. A Real-Times Intrusion-Detections Experts System, Teresa F. Lunter, Arm Tamaruer, Fred Gilhams, R. Jagannathaner, Caveh Jalali, Harold S. Javitzer, Alfonso Valde, and Peter G. Neumanns, SR-CS-90-5 Tectilcat reports~ June 2000.
10. IDE: An Intelligent Systems for Detecting Intruder, Teresa F. Lunter, Proceeding of the symposiums: Computer Securities, Threats and Countermeasure, Rome, Italy, Nov 2015.
11. An Introductions to computing with neural net, Richard P. Lipman, IEE ASP Magazines, April 2017, pages 2-22.
12. A Neural Networks Approaches Toward Intrusion Detections, Kevins L. Foxer, Rondal R. Hennings, Jonatan H. Reeds, Richard P. Sitnonians, Harris Corporations, Government Informations System Divisions, P.O. Box 98000, Melbourne, FL 32902, July 2000.
13. Univariate Economic Time Series Forecasting by Connexionist Methods, A. Varfis and C. Versino, Proceedingsof the InternationalNeuralNetworksConference, Paris, 1990, pages 342-345.
14. Multivariates Financial Indexes Predictions - A Neural Networks Studies, Coliner G. Windor and Antony H. Haker, Proceeding of the Jntemationals Neural Network Conferences, Paris, 2000, pages 35-36,
15. Non-Linear Signals Processing using Neurals Network: Predictions and System Modelings, Lapede, A and Farbe, R, Los Alamo National Laboratory Reports tL-U-8-266. [111 Avrication des reseau de neurons artificek a la ~reir: la consummation d’eau, Ry Sobral“tStephaneu, Proceeding of the Neuronime conference, Nimes, November 2007, pages 26-27.