УДК 69.05

СЕТЕВАЯ БЕЗОПАСНОСТЬ – ОБНОВЛЕННАЯ ПЕРСПЕКТИВА

♦♦♦♦♦

NETWORK SECURITY – AN UPDATED PERSPECTIVE

Тотухов Константин Евгеньевич
кандидат технических наук,
доцент кафедры «Информационные системы
и программирование»,
Кубанский государственный технологический университет

Черненко Михаил Константинович
студент,
Институт компьютерных систем
и информационной безопасности,
Кубанский государственный технологический университет
mr.tchernenko2015@yandex.ru

Раджабов Азамат Олимжонович
студент,
Институт компьютерных систем
и информационной безопасности,
Кубанский государственный технологический университет
radzhabov.azamat00@mail.ru

Аннотация. В данной обзорной статье рассматривается обновленная перспектива сетевой безопасности. Сетевая безопасность – это специализированная область, состоящая из положений и политик для предотвращения и мониторинга несанкционированного доступа, неправильного использования, изменения или отказа в использовании компьютерной сети и доступных по сети ресурсов, а также обеспечения их доступности посредством надлежащих процедур. Многие устройства безопасности разрабатываются и развертываются для защиты от киберугроз и предотвратить непреднамеренные нарушения данных. Несмотря на все эти усилия, «золотой век» киберпреступности продолжается, так как организации во всем мире по-прежнему происходят утечки данных и атаки на систему безопасности. С какими угрозами мы сталкиваемся сегодня? Как с этими угрозами нужно бороться? Целью данной статьи является представление обновленной перспективы сетевой безопасности для организаций и исследователей на местах и представить некоторые рекомендации по решению нынешней ситуации в области безопасности угрозы.

Ключевые слова: кибератаки, утечки данных, вторжения, безопасность сети, разведывательные данные по вопросам безопасности, угрозы безопасности.

Totukhov Konstantin Evgenyevich
Candidate of Technical Sciences,
Associate Professor of the department «Information Systems and programming",
Kuban State Technological University

Chernenko Mikhail Konstantinovich
Student,
Institute of Computer Systems
and information security,
Kuban State Technological University
mr.tchernenko2015@yandex.ru

Rajabov Azamat Olimzhonovich
Student,
Institute of Computer Systems
and information security,
Kuban State Technological University
radzhabov.azamat00@mail.ru

Annotation. This overview article provides an updated perspective on network security. Network security is a specialized field consisting of the provisions and policies to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources as well as ensuring their availability through proper procedures. Many security devices are being developed and deployed to defend against cyber threats and to prevent unintended data breaches. In spite of all these efforts, the 'golden age' of cyber crime continues, as organizations.

Keywords: cyber attacks, data breaches, intrusions, network security, security intelligence, security threats.

1 Введение

В нынешнюю эпоху наблюдается огромный рост сети «Интернет» с точки зрения ее использования и ресурсов. Почти все крупные коммерческие организации, учебные заведения, правительственные учреждения и частные лица зависят от Интернета для предоставление своих услуг. Большинство коммерческих организаций обмениваются информацией со своими сотрудниками и клиенты через Интернет. Учебные заведения: загрузка материалов исследования и результатов исследования по Интернет для скорейшего распространения информации. Правительства предостав-

ляют информацию гражданам через Интернет. Физические лица используют Интернет для доступа к информация, интернет-покупки и общение с другими через электронные письма, социальные сети и т.д. Таким образом, Интернет предоставляет платформу для запуска служб и хранения конфиденциальная информация коммерческих организаций, учебных заведений и правительств. Интернет также обслуживает потребности отдельных лиц путем предоставления соответствующей информации и средств связи. Поэтому плавность управления Интернетом и поддержание целостности, доступности и конфиденциальности информации Интернета – наиболее важные аспекты роста информационных организаций.

Кибератака – это преднамеренная эксплуатация компьютерных систем, технологических сетей и предприятий. Кибератаки используют большой код для изменения компьютерного кода, логики или данных в деструктивных последствиях это может поставить под угрозу информационную безопасность. Такие уязвимости могут быть видны в течение дней или недель, пока не будут исправлены и предоставляет больше шансов злоумышленникам использовать их. Для примера большинство инфекций происходит через «наборы эксплойта» (заражение компьютеров пользователей уязвимостью без их знания). Например, более 90 % из них через уязвимости Java в браузерах (PandaLabs, 2013). Сетевые устройства безопасности состоят из одной или нескольких функций безопасности, включая брандмауэр, системы предотвращения/обнаружения вторжений (IPS/IDS), потерю данных функции предотвращения (DLP) и фильтрации безопасности контента – защита от нежелательной почты, защита от вирусов или фильтрация URL-адресов. Индустрия сталкивается с проблемами быстро меняющихся тенденций атаки Интернет-ресурсов, неспособность традиционных методов для защиты интернет-ресурсов от различных атак, и предубеждения отдельных приемов в сторону конкретной атаки. Разработка эффективных методов, политики безопасности и обеспечение их соблюдения необходимы для обеспечения безопасности ценных материалов от атак.

2 Кибератаки и их принципы

Создание вредоносных программ фиксирует самое большое количество троянских коней в истории, атаки в соцсетях, киберпреступность и кибервойна повсюду. Кибератаки можно разделить на четыре категории, описанные ниже (изображено на рис. 1).

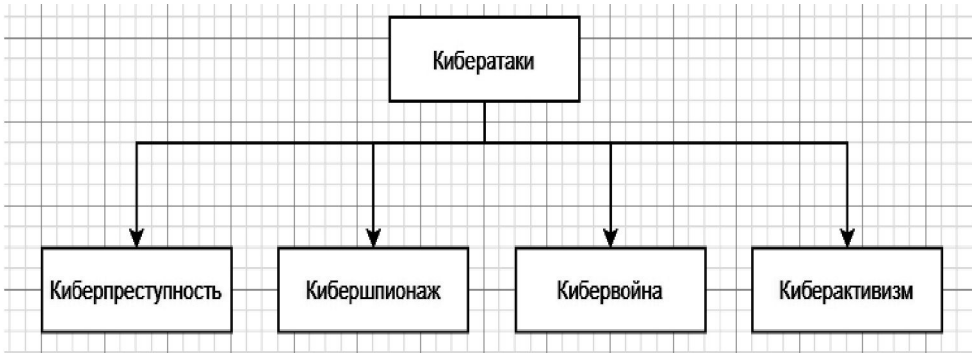

Рисунок 1 – Классификация кибератак

Киберпреступность:

Как правило, под киберпреступлениями понимаются злонамеренные действия по блокировке, считыванию или вмешательству в работу киберуслуг. Множественные принципы информационной безопасности, включая конфиденциальность, целостность и доступность, могут быть скомпрометированы в результате такого типа кибератак. Мотивацией киберпреступников является получение экономической выгоды, компрометацию кибернетической инфраструктуры (например, в кибервойны) и удовлетворенности собой. Большинство киберпреступлений, совершенных в реальном мире, совершаются через онлайн-компьютеры. Как правило, цель киберпреступников – получить доступ к компьютерам жертв, интернет-ресурсам и учетным данным. Как только они

получают доступ к ресурсам жертв любыми способами, эти скомпрометированные ресурсы могут быть использованы для каждой формы любой вредоносной деятельности. Киберпреступления продолжаются ежедневно в реальном мире и будут продолжаться из-за огромных прибылей за их спиной и наличия киберинструментов для совершения этих преступлений.

Кибершпионаж:

Кибершпионаж предполагает кражу информации. Информация может быть украдена киберпреступниками для получения доступа к компьютерной системе или сети. Здесь киберпреступники могут нарушить доверчивость и целостность информации систем. Как правило, преступники работают в течение длительного времени, чтобы получить контроль над системой или доступ к ней и просмотреть имеющуюся онлайн-информацию и другие политики безопасности. Эти преступники, как правило, технически здоровые люди и их трудно обнаружить. Несмотря на то, что силы безопасности лучше подготовлены к борьбе с этим видом преступлений, они по-прежнему ограничены отсутствием границ в Интернете. Полиция может действовать только в пределах своей юрисдикции, в то время как кибер-мошенник может совершить нападение из страны A, украсть данные у граждан страны B, отправить украденные данные на сервер, расположенный в стране C и может проживать в стране D. Это можно сделать всего за несколько кликов, в то время как скоординированные действия сил безопасности в различных странах могут занять месяцы. По этой причине киберпреступники до сих пор живут собственной золотой эпохой. Конфиденциальная информация компаний тем или иным образом делится с другими, поэтому ее нужно защищать от кибершпионажных атак.

Кибервойна:

Кибервойна направлена на отключение или уничтожение компьютерных систем. Как правило, для нацеливания на систему разрабатывается компьютерная программа, известная как кибероружие. Этот тип атаки нарушает доступность и/или целостность системы. Мы можем думать, что домашние пользователи подвергаются наибольшему риску, помните, что обновление приложений, которое необходимо для защиты от этих типов атак, является очень сложным процессом в компаниях, где обновление всех компьютеров должно координироваться. В то же время важно обеспечить правильную работу всех приложений, используемых в компании. Это делает процессы обновления медленными, что открывает окно, которое используется для кражи информации в целом и запуска целевых атак в поисках конфиденциальных данных

Киберактивизм:

Киберактивизм – новейший класс киберпреступности. Это способ использования интернет-технологий общения и коммуникации для создания, эксплуатации и управления активизмом любого типа. Он использует рабочие инструменты и платформы социальных сетей для обмена и трансляции сообщений, а также. Эти платформы включают Twitter, Facebook, LinkedIn, YouTube и другие популярные и нишевые социальные сети. Обманывать пользователей для совместной работы, чтобы заразить их компьютеры и украсть их данные – это простая задача, так как нет приложений для защиты пользователей от себя. В этом контексте использование социальных сетей (Facebook, Twitter и т.д.), где сотни миллионов пользователей обмениваются информацией, во многих случаях персональными данными, делает их предпочтительным местом охоты для обмана пользователей. Например, электронные активисты используют электронные петиции, подписанные числом последователей, прежде чем они будут направлены в правительственные и законодательные органы. Но, для злонамеренных пользователей и технически здравых людей этого недостаточно. Они протестуют против своих компаний, перенаправляют огромное количество трафика на вебсайт компании (DoS-атака), делают большое количество запросов на сервер компании, чтобы отказать им, извлекают личную информацию администраторов компании, чтобы смутить их и получить доступ к политикам компании, чтобы нанести ущерб репутации компании и многому другому.

В таблице 1 представлены различные принципы кибератак и информационной безопасности, которые могут быть скомпрометированы.

Таблица 1 – Кибератаки и принципы информационной безопасности

3 Заключение

В настоящем одной только технологии недостаточно для обеспечения безопасности наших ценных интернет-ресурсов. К сожалению, нет единого решения для обеспечения безопасности от всех потенциальных угроз. Но интегрировав многоуровневую систему безопасности по всей сети, можно по крайней мере получить хорошие шансы на выявление и изоляцию атак до их распространения. Как никогда, кажется, что даже в чувствительной среде было реализовано небольшое подмножество механизма защиты. Даже в современных антивирусах и IDS отсутствует обнаружение APT. Методы обнаружения обрабатывают огромное количество данных аудита, содержащих несущественные и избыточные элементы, что приводит к дополнительным вычислительным затратам. Дополнительные вычислительные издержки приводят к потере возможностей IDS в реальном времени. Использование соответствующих методов выбора признаков наряду с методами на основе ИИ может уменьшить вычислительные накладные расходы. Политика безопасности, отвечающая требованиям соответствующей организации, должна быть четко определена для предотвращения кибератак. В этой политике должны быть четко определены пути безопасного проведения различных операций. Особое внимание следует уделять защите сетей от уязвимостей операционной системы и приложений. Пользователи должны быть вовлечены в обеспечение безопасности соответствующих организаций. Поскольку они отвечают за использование и обмен конфиденциальными данными организаций. Они должны пройти обучение по различным угрозам для своих организаций и тому, как их меры предосторожности могут помочь предотвратить нападения.

Настоящее время само по себе полно проблем в мире сетевой безопасности. Все, похоже, указывает на то, что число угроз, с которыми придется столкнуться пользователям, будет продолжать расти, поэтому сейчас как никогда важна защита: Наличие хорошей политики безопасности, поддержание продуктов безопасности (таких как антивирус, антиспам) в актуальном состоянии и обеспечение соблюдения политики безопасности являются лучшими способами избежать стать жертвой киберпреступника.

Литература

1. Берова Д.М. Кибератаки как угроза информационной безопасности. [Электронный ресурс]. – URL : https://cyberleninka.ru/article/n/kiberataki-kak-ugroza-informatsionnoy-bezopasnosti.

2. Denman S. Why multi-layered security is still the best defence // Network Security. – 2012. – № 3. – С. 5–7.

3. Hilbert E. Living with cybercrime // Network Security. – 2013. – № 11. – С. 15.

References

1. Berova Ju.M. Cyberattacks as a Threat to Information Security. [Electronic resource]. – URL : https://cyberleninka.ru/article/n/kiberataki-kak-ugroza-informatsionnoy-bezopasnosti.

2. Denman S. Why multi-layered security is still the best defense // Network Security. – 2012. – № 3. – P. 5–7.

3. Hilbert E. Living with cybercrime // Network Security. – 2013. – № 11. – P. 15.