7universum.com
UNIVERSUM:
ТЕХНИЧЕСКИЕ НАУКИ

UNIVERSUM:
ТЕХНИЧЕСКИЕ НАУКИ

Научный журнал
Издается ежемесячно с декабря 2013 года
Является печатной версией сетевого журнала
Universum: технические науки

Выпуск: 2(95)

Февраль 2022

Часть 1

Москва
2022

УДК 62/64+66/69
ББК 3
U55

U55 Universum: технические науки: научный журнал. – № 2(95). Часть 1. М., Изд. «МЦНО», 2022. – 72 с. – Электрон. версия печ. публ. – http://7universum.com/ru/tech/archive/category/295

ISSN : 2311-5122

DOI: 10.32743/UniTech.2022.95.2-1

Учредитель и издатель: ООО «МЦНО»

ББК 3

Содержание

СЕТЕВЫЕ АТАКИ И ИСПОЛЬЗОВАНИЕ ЗАЩИТЫ ОТ НИХ

Турдиева Гавхар Саидовна
ст. преподаватель,
Бухарского государственного университета,
Республика Узбекистан, г. Бухара
E-mail: evrikiy@list.ru

NETWORK ATTACKS AND THEIR USE OF PROTECTION

Gavhar Turdieva
Senior Lecturer,
Bukhara State University,
Respublika Uzbekistan, Bukhara

АННОТАЦИЯ

Если сеть не защищена должным образом, компания рискует потерять не только данные, но и доверие и репутацию на рынке при атаке. Если компания не может должным образом защитить свою сеть, все усилия компании по продвижению и привлечению трафика на сайт могут быть внезапно сорваны. В статье анализируются лучшие практики и различные виды сетевой безопасности.

ABSTRACT

If the network is not adequately protected, the company runs the risk of losing not only data, but also trust and reputation in the market when an attack occurs. If a company is unable to properly protect its network, all of the company's efforts to promote and generate traffic to the site may suddenly be thwarted. The article analyzes best practices and different types of network security.

Ключевые слова: сетевые атаки, сетевая безопасность, брандмауэр, уязвимость.
Keywords: network attacks, network security, firewall, vulnerability

---

Новые цифровые технологии открывают новые возможности для анализа больших данных, что может привести к киберугрозам со стороны кибер-захватчиков и террористов. Сегодня Интернет знает о пользователе больше, чем его близкие родственники, что грозит хищением личной информации и использованием ее в корыстных целях.

Во всем мире более половины малых и средних предприятий и индивидуальных предпринимателей столкнулись с кибербезопасностью.

Эти организации опасаются, что риск кибератак высок из-за нехватки ресурсов и опыта в области кибербезопасности. Эта проблема обострилась в эпоху COVID-19 из-за перехода на цифровые технологии. Наиболее распространенными методами атак, с которыми сталкивались эти организации, были вредоносное ПО/вирусы (24%), повреждение данных (16%) и фишинговые атаки (15%). Девять из 10 респондентов (88%) заявили, что у них есть по крайней мере одна форма кибербезопасности, такая как антивирусное программное обеспечение, брандмауэр или многофакторная аутентификация, а 70% заявили, что они слишком уверены или переоценивают свои процедуры кибербезопасности. знать, что устройство надежно.

Сетевые атаки — это несанкционированные действия с цифровыми активами в сети организации. Злоумышленники обычно проводят сетевые атаки, чтобы изменить, удалить или украсть личную информацию. В сетевых атаках преступники нацелены на периметры сети, чтобы получить доступ к внутренним системам. Существует два основных типа сетевых атак: пассивные и активные. При пассивных сетевых атаках злоумышленники входят в сети без разрешения, контролируют и крадут личную информацию без внесения каких-либо изменений. Активные сетевые атаки включают изменение, шифрование или повреждение данных.

Количество и внешний вид атак с использованием сети растет очень быстро. Постоянные атаки — серьезная проблема для всего компьютерного мира. Именно поэтому организации тратят огромные суммы на обеспечение сетевой безопасности. Проблемы сетевой безопасности влияют на удобство использования, конфиденциальность и целостность информации, доступной в организации. Злоумышленники пытаются выявить бреши в безопасности, связанной с технологиями. В свою очередь, это требует, чтобы системный администратор был в курсе новых атак, которые появляются в сети.

Построение сети — простая задача, а обеспечение ее безопасности — сложная задача. Причина в том, что злоумышленник пытается обнаружить уязвимости в системе с помощью различных инструментов.

Сеть организации также может подвергаться различным атакам изнутри. Атака изнутри обычно более опасна, чем атака снаружи.

Библиографическое описание: Турдиева Г.С. СЕТЕВЫЕ АТАКИ И ИСПОЛЬЗОВАНИЕ ЗАЩИТЫ ОТ НИХ // Universum: технические науки: электрон. научн. журн. 2022. 2(95). URL: https://7universum.com/ru/tech/archive/item/13106

Поэтому организация должна ежедневно выполнять важную задачу, такую как мониторинг и обнаружение сетевых атак.

Следующие факторы в настоящее время способствуют увеличению сетевых проблем:

Устройство или программный инструмент настроены неправильно. Уязвимости безопасности обычно вызваны неправильной настройкой устройства или программного обеспечения в сети. Например, использование неправильно настроенного или не имеющего шифрования протокола приведет к раскрытию конфиденциальной информации, пересылаемой по сети. Неправильно настроенное устройство может дать злоумышленнику доступ к системе или сети. Неправильно настроенный программный инструмент может привести к несанкционированному использованию приложения или программного обеспечения.

Небезопасный и плохой дизайн сети. Сеть, спроектированная неправильно и небезопасно, может столкнуться с различными угрозами и возможностью потери данных. Например, если технологии брандмауэра, IDS и виртуальной частной сети (VPN) реализованы небезопасно, они могут сделать сеть уязвимой для различных угроз.

Врожденная технологическая уязвимость. Если устройство или программный инструмент не может справиться с определенными типами сетевых атак, то оно будет уязвимо для этих атак. Многие устройства, приложения или веб-браузеры нетерпимы к атаке, побуждающей их отказаться от службы, или к нападениям со стороны человека. Если в системах используется более старый веб-браузер, эти системы будут более уязвимы для распределенных атак. Если системы не обновлены, может быть достаточно небольшой троянской атаки, чтобы очистить машину пользователя.

Невежество пользователей. Халатность последних пользователей сети может оказать серьезное влияние на безопасность сети. Могут возникнуть серьезные проблемы с безопасностью, такие как потеря данных, утечка в результате действий человека. Злоумышленники также используют технологии социальной инженерии для сбора информации о пользователях.

Умышленные действия пользователей. Уволенный сотрудник может по-прежнему использовать распределенный диск. В этом случае это приведет к утечке конфиденциальной информации организации. Такая ситуация расценивается как преднамеренные действия пользователей.

Сетевые угрозы обычно делятся на два типа: внутренние угрозы и внешние угрозы.

Внутренние угрозы. 80% преступлений, связанных с компьютером или Интернетом, являются внутренними атаками. Эти атаки могут быть осуществлены обиженными, злонамеренными сотрудниками внутри организации. Большинство этих атак осуществляются привилегированными пользователями сети.

Внутренние атаки могут представлять более серьезную угрозу, чем внешние атаки. Основной причиной этого является падение сети, осуществляющей внутреннюю атаку, политика безопасности и знание организацией законодательства.

Внешние угрозы. Внешние атаки являются результатом уже существующей в сети уязвимости. Злоумышленник может осуществлять эти атаки просто ради интереса, материальной выгоды или для дискредитации организации. При этом нападающий обладает высокой квалификацией и может работать в команде. При проведении атаки используются специальные технологии, наблюдается долговременная готовность. При этом атаки осуществляются без помощи внутреннего персонала. Некоторые внешние атаки включают атаки на основе злоумышленников и вирусов, атаки на основе паролей, атаки на основе вредоносных сообщений и атаки на основе операционной системы.

Внешние угрозы принято делить на два типа: структурированные и несистематические внешние угрозы.

Систематизированная внешняя угроза. Систематизированные внешние угрозы осуществляются высококвалифицированными лицами. Эти люди смогут быстро определить существующую уязвимость в сети и использовать ее в своих интересах. Эти лица или группы лиц обычно причастны к совершению крупных киберпреступлений.

Бессистемная внешняя угроза. Бессистемные внешние угрозы обычно осуществляются неквалифицированными лицами с использованием различных готовых хакерских инструментов и скриптов. Эти типы атак обычно выполняются отдельными лицами, чтобы проверить свои способности или проверить, есть ли уязвимость в организации.

Как использовать антивирусное программное обеспечение:

Антивирусное программное обеспечение защищает ваше устройство от вирусов, которые могут удалять данные, замедлять или выключать ваше устройство или позволять спамерам отправлять электронные письма через вашу учетную запись. Антивирусная защита сканирует файлы и нежелательные сообщения электронной почты на наличие вирусов, а затем удаляет любые вредоносные объекты. Вам необходимо постоянно обновлять антивирусное программное обеспечение, чтобы справляться с последними «ошибками», которые распространяются в Интернете. Большинство антивирусных программ имеют возможность автоматически загружать обновления, когда вы находитесь в сети. Кроме того, убедитесь, что программное обеспечение постоянно запущено и сканирует систему на наличие вирусов, особенно если вы загружаете файлы из Интернета или проверяете свою электронную почту. Установите антивирусную программу для ежедневного сканирования на наличие вирусов. Вы также должны тщательно сканировать свою систему, по крайней мере, два раза в месяц [1].

Шпионское ПО — это программное обеспечение, устанавливаемое без вашего ведома или согласия, которое может отслеживать ваши действия в

Интернете и собирать личную информацию, пока вы находитесь в сети. Некоторые программы-шпионы, называемые кейлоггерами, будут записывать все, что вы вводите, включая ваши пароли и финансовую информацию. Признаки того, что ваше устройство могло быть скомпрометировано шпионским ПО, включают внезапное увеличение рекламы, посещение веб-сайтов, которые вы не хотите посещать, и общее снижение производительности. Защита от шпионского ПО включена в некоторые антивирусные программы. Инструкции по активации функций защиты от программ-шпионов см. в документации к антивирусному программному обеспечению. Вы можете купить отдельное шпионское ПО. Как использовать Брандмауэр.

Брандмауэр — это программа или оборудование, которое блокирует доступ хакеров к вашему компьютеру и его использование. Подобно тому, как некоторые телепродавцы автоматически набирают случайные телефонные номера, хакеры ищут информацию в Интернете. Они отправляют экзо-запросы (вызовы) на тысячи компьютеров и ждут ответов. Брандмауэры не позволяют вашему компьютеру отвечать на эти случайные вызовы. Брандмауэр блокирует связь с источниками, которые вы не разрешаете. Это особенно важно, если у вас есть высокоскоростное подключение к Интернету, такое как DSL или кабель. Некоторые операционные системы имеют встроенные брандмауэры, которые можно отключить. Убедитесь, что вы включили брандмауэр. Чтобы быть эффективным, ваш брандмауэр должен быть правильно настроен и регулярно обновляться.

Как выбирать надежные пароли.

Защитите свое устройство и учетные записи от злоумышленников, выбрав пароли, которые трудно угадать. Используйте надежные пароли, состоящие не менее чем из восьми символов, комбинации букв, цифр и специальных символов. Важно не использовать слова, которые легко найти в словаре, или ссылки на личную информацию, например день рождения. Некоторые хакеры используют программы, которые проверяют каждое слово в словаре и легко находят личную информацию, например дату рождения. Попробуйте использовать первую букву каждого слова и фразу, которая поможет вам вспомнить пароль.

Что такое система обнаружения атак?

Это система, которая отслеживает сетевой трафик для обнаружения несанкционированного доступа или активности в сетевой среде. При обнаружении аномалии некоторые системы обнаружения атак/сбоев способны предпринимать определенные действия для предотвращения или смягчения последствий атак.

Эффективная кибербезопасность имеет решающее значение для бизнеса, и она становится все более важной по мере распространения инициатив цифровой трансформации, облачных вычислений и удаленной работы в организациях. Злоумышленники все чаще атакуют подключенные к Интернету системы и плохо защищенные веб-приложения, тем более что все больше людей работают из дома из-за пандемии COVID-19.

Список литературы:

1. Анорбоев А. Преступление киберпреступности: уголовно-правовая и криминологическая характеристика. - Т.: 2020, Журнал правовых исследований. 2- специальный номер. - Б. 300-309.
2. Турдиева Г.С., Шойимов А.С.Основные особенности и функции использования современных облачных служб в системе образования// Вестник науки и образования 2021. № 17 (120).Часть 3. 52-55 стр.
3. Турдиева Г.С. Исползование информационных технологий в сфере туризма // Шойимов А. Научно-методический журнал “ACADEMY” Российский-импакт фактор:0.19. №6 (57). 2020 г.22-24 бет.