Молодёжный вестник НФ БГТУ. 2022. Том 02. № 02 (06)
https://rio-nb-bstu.science

ИНФОРМАТИКА. КРАТКИЕ СООБЩЕНИЯ

doi: 10.51639/2713-0576_2022_2_2_67
УДК 004.056.5
ГРНТИ 20.00.00
ВАК 05.13.19

Адаптивный подход к управлению безопасностью компьютерных сетей

[*] Шагойко М. А., Щемелева Ю. Б.

Филиал Южного федерального университета в г.Геленджике
Россия, Краснодарский край, г.Геленджик, ул.Заставная, 10а

e-mail: [*] shagoyko@sfedu.ru, da-yula@yandex.ru

В данной работе обеспечение безопасности компьютерных сетей ставится как задача, требующая комплексного подхода. Отмечается, что, единоразовые решения не могут обеспечить достаточную степень защиты ввиду постоянного совершенствования способов ее нарушения. Предлагается для обеспечения надежной защиты использовать модель адаптивного управления безопасностью ANS (Adaptive Network Security). Отмечается, что адаптивный подход к безопасности позволит контролировать, обнаруживать риски безопасности и реагировать на них в режиме реального времени, на основе управляемых процессов. Разработана структура адаптивной системы управления в компьютерных сетях. Отмечено, что оценка риска состоит в выявлении и ранжировании уязвимостей (по степени серьёзности ущерба); подсистем сети (по степени критичности); угроз (исходя из вероятности их реализации). На основе данных предположений построена номограмма для оценки рисков.

Ключевые слова: безопасность компьютерных сетей, адаптивная система обеспечения безопасности.

Актуальность

Информационная безопасность– это комплекс действий, направленных на решение проблемы защиты информационной среды. Для защиты информации необходимо соблюдать главные принципы: целостность, конфиденциальность, доступность, подлинность (аутентичность) и неотрекаемость.

Разрабатывая модель системы информационной безопасности для конкретной организации, сначала необходимо обозначить, какие источники информации следует защитить, какова цель получения доступа к защищаемой информации, что является источником конфиденциальной информации, как защититься от несанкционированных попыток воздействия на систему. На втором этапе разрабатывают систему защиты. Система строится сразу по нескольким направлениям, на нескольких уровнях, которые взаимодействуют друг с другом для обеспечения надежного контроля информации: правовой уровень, организационный уровень, технический уровень. Третий этап – это поддержка работоспособности системы, регулярный контроль, скрининг и управление рисками.

Постоянное совершение способов и методов угроз информационной безопасности порождает актуальность мониторинга и совершенствования средств защиты компьютерных сетей.

Целью настоящей работы является постановка задачи обеспечения адаптивного подхода к обеспечению безопасности компьютерных сетей.

Молодёжный вестник НФ БГТУ. 2022. Том 02. № 02 (06)
https://rio-nb-bstu.science

Для реализации указанной цели нами даны ответы на вопросы: каковы основные способы утечки информации в компьютерных сетях, как осуществить адаптивный подход к управлению безопасностью.

Основная часть

Для того чтобы знать, как защитить информацию в сетях передачи данных, необходимо определить пути, по которым эта информация передается и через которые она может попасть в третьи руки. Можно выделить следующие способы утечки информации в компьютерной сети:
- утечка через физический канал (кабели). Наиболее дорогостоящий канал передачи (и потому доступен крупным предприятиям, военным организациям и т. п.). Обладает самой высокой защищённостью. Для получения доступа к передаваемой информации необходим «взлом» начальной либо конечной точки, или же «врезка» в канал передачи данных. И то, и другое трудноосуществимо и поддаётся идентификации. Стоимость реализации данного способа передачи данных можно уменьшить, арендовав физический канал, однако при этом увеличится его уязвимость;
- утечка при передаче данных через сеть Интернет. Весьма небезопасный канал передачи данных, которые могут быть подвергнуты рискам искажения, перехвата, потери. Эти риски не зависят от воли третьих лиц, а носят случайный характер, среди них можно выделить человеческий фактор, ошибки программирования, пресловутый человеческий фактор и прочее;
-утечка через мессенджеры. Внезапно, не самый худший канал передачи данных, т. к. каждый мессенджер имеет свою сложную систему авторизации и определённые хорошо защищённые протоколы передачи данных. Поэтому данные тяжело перехватить.
- утечка по беспроводным сетям. Наибольшая вероятность потерять передаваемые данные существует в Wi-fi сетях, особенно незащищенных, так как в настройки маршрутизатора не имеют должной защиты, кроме того пользователи, как правило, не меняют стандартные настройки WI-fi и тем более даже не предпринимают хоть какие-то меры предосторожности работая в данных сетях.
Таким образом, обеспечение безопасности компьютерных сетей видится задачей, требующей комплексного подхода. Кроме того, единоразовые решения не могут обеспечить достаточную степень защиты ввиду постоянного совершенствования способов ее нарушения.

Решение

Одним из вариантов решения, способных стать основой для обеспечения всеобъемлющей защиты, может стать модель адаптивного управления безопасностью ANS (Adaptive Network Security). Подобная модель разработана компанией Компания ISS (Internet Security Systems). Адаптивный подход к безопасности позволяет контролировать, обнаруживать риски безопасности и реагировать на них в режиме реального времени, на основе управляемых процессов. Основными составляющими адаптивной системы ANS являются технологии анализа защищенности (security assessment); технологии обнаружения атак (intrusion detection); технологии управления рисками (risk management), как показано на рис. 1.
Оценка риска состоит в выявлении и ранжировании уязвимостей (по степени серьёзности ущерба); подсистем сети (по степени критичности); угроз (исходя из вероятности их реализации). Следует заметить, что наиболее вероятные угрозы, являясь наиболее доступными даже для неопытного хакера, приносят наименьший ущерб. При этом серьёзность ущерба при любом взломе является величиной, отличной от нуля. Это позволяет представить описанную взаимосвязь в виде номограммы, изображенной на рис. 2.

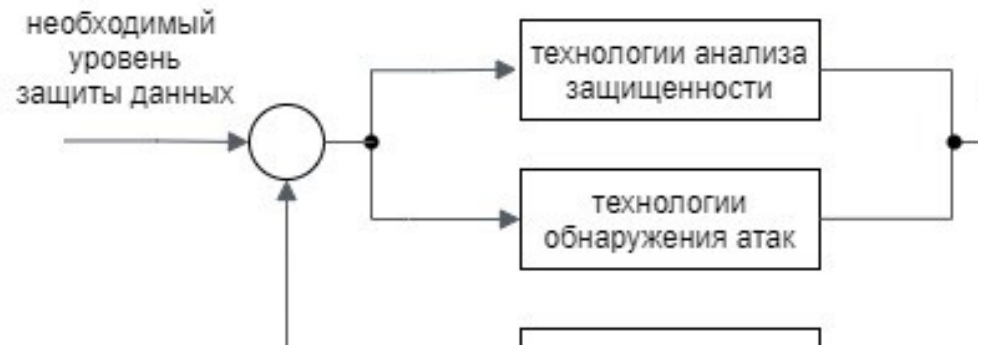

Рис. 1. Структура адаптивной системы управления безопасностью в компьютерных сетях

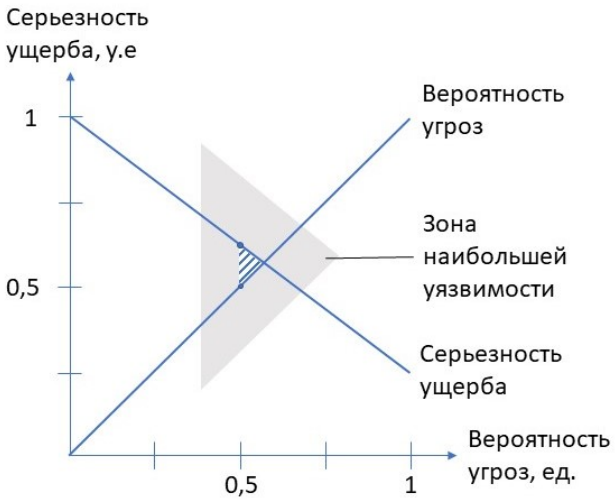

Рис. 2.Номограмма для оценки риска

Заключение

В адаптивной системе управления безопасностью сети постоянно проводится анализ защищённости. Это позволяет оперативно находить слабые места сети, через которые возможна атака на сеть, прогнозировать точку нанесения «удара». Даже простой анализ в рамках управления рисками позволяет выявить следующие проблемы: слабые пароли; «двери» в систему (backdoor) и программы вида «троянский конь»; отсутствие необходимых патчей и обновлений в системе; неверная настройка межсетевых экранов.

Адаптивный компонент системы безопасности отвечает за модификацию анализа защищенности, исходя из известных ей угроз на текущее время и путях их «входа» в систему, т.е. уязвимостей. Адаптация может иметь разные виды реакций на воздействия в системе: отсылка уведомлений администратору; мгновенное отключение узла\пользователя откуда идёт атака; реконфигурация скомпрометировавшего себя сетевого оборудования; отсылка отчёта по текущим уязвимостям администратору и способам их устранения.

Использование адаптивной системы повышает общую защиту подотчётной системы или сети, не отбрасывая уже имеющиеся механизмы защиты (разграничение доступа, аутентификация и т.п.), а фактически расширяя их.

Конфликт интересов

Авторы статьи заявляют, что у них нет конфликта интересов по материалам данной статьи с третьими лицами на момент подачи статьи в редакцию журнала, и им ничего не известно о возможных конфликтах интересов в настоящем со стороны третьих лиц.

Молодёжный вестник НФ БГТУ. 2022. Том 02. № 02 (06)
https://rio-nb-bstu.science

Список литературы

1. Шаньгин В. Ф. Защита компьютерной информации : учебное пособие / В. Ф. Шаньгин. — Москва : ДМК Пресс, 2010. — 544 с. — ISBN 978-5-94074-518-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/1122 (дата обращения: 26.05.2021). — Режим доступа: для авториз. пользователей.
2. Коммерческая тайна предприятия — что это, отличие от конфиденциальной информации. (электронный ресурс) https://okarb.ru/oplata-truda/kommercheskaya-tajna-predpriyatiya-chto-eto-otlichie-ot-konfidentsialnoj-informatsii.html (дата обращения 10.05.2021)
3. Проблемы автоматизации. Региональное управление. Связь и автоматика (ПАРУСА-2018) Сборник трудов VII Всероссийской научной конференции молодых ученых, аспирантов и студентов: в 2 томах / Составители: Ю. Б. Щемелева, С. В. Кирильчик. 2018. Том 1.
4. Обеспечение комплексной информационной безопасности в современном офисе. Григорьян И. Г., Григорьян Л. Г., Щемелева Ю. Б.В сборнике: Проблемы автоматизации. Региональное управление. Связь и акустика. сборник трудов X Всероссийской научной конференции и молодежного научного форума в рамках мероприятий, посвященных году Науки и технологий в Российской Федерации. Ростов-на-Дону, 2021. С. 409–413.

Adaptive approach to computer network security management

Shagoyko M. A., Shchemeleva Y. B.

Branch of the Southern Federal University in Gelendzhik
Russia, Krasnodar Territory, Gelendzhik, Zastavnaya str, 10a

In this paper, ensuring the security of computer networks is set as a task that requires an integrated approach. It is noted that one-time solutions cannot provide a sufficient degree of protection due to the constant improvement of ways to violate it. It is proposed to use the adaptive security management model ANS (Adaptive Network Security) to ensure reliable protection. It is noted that an adaptive approach to security will allow monitoring, detecting security risks and responding to them in real time, based on managed processes. The structure of an adaptive control system in computer networks has been developed. It is noted that the risk assessment consists in identifying and ranking vulnerabilities (according to the severity of damage); network subsystems (according to the degree of criticality); threats (based on the probability of their implementation). Based on these assumptions, a nomogram for risk assessment is constructed.

Keywords: computer network security, adaptive security system.