DOI: 10.58168/CISMP2024_303-306
УДК 004.51

ИСПОЛЬЗОВАНИЕ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ДЛЯ ОБНАРУЖЕНИЯ УЯЗВИМОСТЕЙ ПРИ ПРОВЕДЕНИИ АУДИТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Ю.Ю. Громов[1], П.И. Карасев[2], Ф.М. Пыршев[1]

[1]ФГБОУ ВО «Тамбовский государственный технический университет»
[2]МИРЭА - Российский технологический университет

Аннотация. Статья позволит подробно рассмотреть тему аудита информационной безопасности с использованием сетевых анализаторов и тестов на проникновение, а также подчеркнуть важность этого процесса для организаций любого масштаба и сферы деятельности в условиях развития сетевых технологий и сложившейся геополитической ситуации.

Ключевые слова: тестирование на проникновение, сетевые анализаторы, уязвимость, кибератаки, информационная безопасность.

USE OF AUTOMATED SYSTEMS FOR VULNERABILITY DETECTION DURING INFORMATION SECURITY AUDITS

Y.Y. Gromov [1], P.I. Karasev[2], F.M. Pyrshev[1]

[1]Tambov State Technical University
[2]MIREA - Russian Technological University

Abstract. The article will allow us to consider in detail the topic of information security audit using network analyzers and penetration tests, as well as to emphasize the importance of this process for organizations of any scale and field of activity in the context of the development of network technologies and the current geopolitical situation.

Keywords: penetration testing, network analyzers, vulnerability, cyber-attacks, information security.

Актуальность аудита информационной безопасности в современных условиях обусловлена ростом числа кибератак, с каждым годом количество кибератак увеличивается, что делает информационную безопасность одной из главных забот для бизнеса и государственных учреждений.

Рисунок 1 – Динамика роста числа кибератак по кварталам

Развитие технологий приводит к усложнению ИТ-инфраструктур, что требует более тщательного подхода к обеспечению безопасности. Также на законодательном уровне существуют требования к защите персональных данных и другой информации, вследствие чего аудит помогает убедиться в соответствии системы защиты этим требованиям.

Не малую роль для различных компаний играют репутационные риски. Утечки данных и кибератаки могут нанести серьезный ущерб репутации, что может привести к потере клиентов и инвесторов. Таким образом, аудит информационной безопасности остается актуальным и необходимым инструментом для обеспечения безопасности данных и защиты интересов компаний и организаций в условиях постоянно растущих киберугроз [1].

В само понятие аудита информационной безопасности входит процесс получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности автоматизированной системы в соответствии с определёнными критериями и показателями безопасности.

Задачами аудита является анализ текущего состояния информационной безопасности организации с последующим выявлением уязвимостей и потенциальных угроз, разработкой рекомендаций по улучшению системы информационной безопасности и контроль за их выполнением. Таким образом аудит информационной безопасности дает возможность организациям оценить готовность системы и персонала к возможным атакам, а также выявить слабые места и устранить их.

Аудит информационной безопасности включает в себя различные методы и подходы, направленные на оценку текущего состояния системы защиты информации и выявление возможных уязвимостей. Среди основных методов можно выделить: интервьюирование сотрудников, анализ документации и политик безопасности, использование сетевых анализаторов, тестирование на проникновение и сканирование уязвимостей. Далее в данной статье будут более подробно рассмотрены методы, связанные с компьютерными системами и сетевой безопасностью.

Сетевые анализаторы – это инструменты, предназначенные для анализа сетевого трафика в реальном времени. Они выполняют функции, аналогичные сетевым мониторам, но дополнительно помогают выявлять причины неполадок в сети и устранять их. Они бывают нескольких видов:

Анализаторы протоколов (Protocol Analyzers) – инструменты, позволяющие просматривать и анализировать данные, передаваемые по сети, на уровне отдельных протоколов. Примеры: Wireshark, TCPDump.

Сетевые мониторы (Network Monitors) – обеспечивают мониторинг сетевого трафика, но не всегда предоставляют детализированный анализ данных. Примеры: Zabbix, Nagios.

Системы обнаружения вторжений (Intrusion Detection Systems, IDS) – специализированы на выявлении несанкционированных действий в сети, таких как попытки взлома. Примеры: Snort, Suricata. [2].

Принцип работы сетевых анализаторов заключается в том, чтобы перехватить весь трафик или его часть, который идет между сервером и клиентом, декодировать его содержимое и структуру, и проанализировать данный трафик на предмет каких-либо подозрительных активностей или аномалий. В следствие чего сетевые анализаторы могут фильтровать трафик, выделяя только интересующее пакеты для дальнейшего анализа, а также создавать отчеты о результатах анализа, которые могут быть использованы для дальнейшей диагностики и устранения проблем.

Тесты на проникновение (пентест) – это метод оценки безопасности компьютерных систем или сетей путем моделирования атаки злоумышленника. Цель пентеста – оценить возможность осуществления атаки и спрогнозировать экономические потери в случае успешного проникновения. Есть внутренний и внешний пентест, первый направлен на оценку безопасности системы со стороны внешнего потенциального злоумышленника, а второй со стороны внутреннего сотрудника, имеющего доступ к системе.

Проведение тестов на проникновение стоит начинать с определения целей и задач теста, с помощью каких инструментов он будет осуществляться и какими методами тестирования выполняться. Далее следует получить как можно больше информации о тестируемой системе, ее структуре и используемых технологиях. Используя полученную информацию об изученной системе, можно приступать к моделированию атаки, что поможет обнаружить уязвимости, оценить их критичность и возможность проведения такой атаки в реальных условиях. По итогу тестирования составляются документы, содержащие описание проведенных тестов, выявленные уязвимости и рекомендации по их устранению, что помогает обеспечить информационную безопасность системы, позволяя предотвратить возможные атаки [3].

Вывод

Таким образом в совокупности использование сетевых анализаторов и тестов н проникновение позволяют аудиторам и специалистам по информационной безопасности получить более детальную картину состояния сетевой системы организации, делая процесс аудита более оптимизированным

и эффективным, что, в свою очередь, позволяет предотвратить потенциальные кибератаки, минимизировать ущерб от уже произошедших инцидентов и поддерживать высокий уровень доверия клиентов и партнеров.

Список литературы

1. Кибербезопасность в 2023–2024 гг.: тренды и прогнозы. Часть третья / // positive technologies : [сайт]. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/kiberbezopasnost-v-2023-2024-gg-trendy-i-prognozy-chast-tretya/ (дата обращения: 09.09.2024).

2. Шарифов, Б.А. Методика проведения аудита с использованием информационных технологий и персональных компьютеров / Б.А. Шарифов // Молодой ученый. – 2021. – № 3 (345). – С. 332-335.

3. Макаренко С.И., Смирнов Г.Е. Анализ стандартов и методик тестирования на проникновение // Системы управления, связи и безопасности. 2020. № 4.

References

1. Cybersecurity in 2023-2024: trends and forecasts. Part three // positive technologies: [website]. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/kiberbezopasnost-v-2023-2024-gg-trendy-i-prognozy-chast-tretya / (date of reference: 09.09.2024).

2. Sharifov, B.A. Audit methodology using information technology and personal computers / B.A. Sharifov. // A young scientist. – 2021. – № 3 (345). – Pp. 332-335.

3. Makarenko S.I., Smirnov G.E. Analysis of standards and methods of penetration testing // Management, communication and security systems. 2020. № 4.