Секция «Круглый стол для школьников «Постигая аудит»»

Выявления уязвимостей и анализ механизмов реализации угроз безопасности

Научный руководитель – Тарасов Иван Владимирович

Угуралиева Карина Давронбековна
E-mail: tiwell28@rambler.ru

ГБОУ «Школа №556», Москва, Днепропетровская ул., 33А
Соавтор: Чаплыгина Анастасия Андреевна, ученица 10 класса,

Аннотация. В данной статье, мы бы хотела кратко и понятно рассказать о том, как выявлять уязвимости разных механизмов безопасности и угрозы для них.

Ключевые слова: угроза, риск, несанкционированное проникновение, злоумышленник, конфиденциальность, защита.

Infrastructure security Management

Annotation. In this article, I would like to briefly and clearly talk about how to identify vulnerabilities of various security mechanisms and threats to them.

Keywords: threat, risk, unauthorized entry, attacker, confidentiality, protection.

Введение

«Меня взломали!» Мы слышим это всякий раз, когда в публикациях знаменитостей находят что-то неприглядное, но иногда их действительно взламывают, и последствия бывают катастрофическими.

Гипотеза. При неэффективной защите информационных систем появляется большой риск взлома.

Цель. Изучить возможности взлома информационных систем и персональных баз данных и способы их защиты.

Задачи.

1. Изучить возможности взлома информационных систем и персональных баз данных и способы их защиты.

2.понять принципы взлома информационных систем.

Предмет исследования. Опасность халатной защиты персональной информации и методы устранения возможности обнаружения уязвимых мест информационных систем.

Актуальность. Информационными системами в наше время пользуются практически все. Они используются в самых разных областях жизни людей, таких как: школы, больницы, бухгалтерия и т.д. Но, увы, из-за своей частой используемости и постоянной нужности, они чаще всего подвергаются взлому. Пока что не существует полностью идеально защищенной программы для хранения персональных или общих данный, поэтому существуют способы выявления угроз безопасности, о которых я хочу вам рассказать.

Выявления уязвимостей и анализ механизмов реализации угроз безопасности

Анализ уязвимостей - это процессы поиска любых угроз, уязвимых точек и рисков потенциального несанкционированного проникновения злоумышленников в информационную систему. Несмотря на дорогостоящие новые методы, опыт использования компьютерных информационных систем показал наличие небольших пробелов и более уязвимых для взлома мест в защите информации. Неизбежным следствием стали огромные расходы и усилия на их защиту. Однако для того, чтобы все предпринятые меры оказались действительно эффективными, необходимо определить, что такое угроза безопасности информации, выявить возможны места утечки информации и пути несанкционированного доступа к защищаемым данным.

Если присутствуют уязвимости, это негативно сказывается на работе всего предприятия, так как оно становится менее защищенным перед недобросовестными конкурентами, это упрощает работу злоумышленников по нанесению вреда и позволяет третьим лицам получить доступ к конфиденциальным данным. Существует 8 самых популярных видов взлома: Bait and Switch, Кража Cookie, Отказ / распределенный отказ в обслуживании, Подслушивание или запись объемного звука, Кейлоггинг, WAP-атаки, Malware и Фишинг.[12] Хоть это и разные методики, смысл у них остается общим - взломать вас ради собственной выгоды или крупного вознаграждения. Сравним взломы персональных данных 2020 и 2021 годов. **Рис. 1. Количество атак в 2020 и 2021 годах**

Вывод. Количество атак в 2021 году увеличилось всего на 6,5% по сравнению с 2020 годом. О замедлении роста числа атак сообщают и в МВД России. На наш взгляд, это связано с тем, что мир адаптировался к новым условиям работы на фоне пандемии коронавируса, а атаки на крупные компании мотивировали топ-менеджеров обращать больше внимания на вопросы, связанные с безопасностью. Доля целевых атак в сравнении с 2020 годом выросла на 4 процентных пункта (п. п.) и составила 74% от общего количества.[12]

В связи с прогрессированием технологий увеличивается риск взлома ваших персональных данных и общих информационных систем. Чтобы справиться с этой проблемой придумывают и создают всё больше и больше различных методик сохранения информации в тайне от злоумышленников, но, помимо их создания, нужно учиться ими пользоваться и грамотно с ними обращаться.

Чтобы провести качественный анализ уязвимостей информационной структуры, необходимо различать виды угроз, которые могут возникнуть в системе конкретной организации. Такие угрозы разделяются на отдельные

I класс

Потенциальный источник угрозы

1. В пределах видимости информационной системы (например, устройства для несанкционированной звукозаписи).
2. Вне зоны видимости ИС (перехват данных в процессе их отправки куда-либо).

II класс

Воздействие на ИС

1. Пассивную угрозу (копирование конфиденциальной информации злоумышленником).

III класс

Метод обеспечения доступа

1. Напрямую (кража паролей).
2. Посредством нестандартных каналов связи (например, уязвимости операционной системы).

Главные цели атаки на ИТ-инфраструктуру компании

1. Получение контроля над ценными ресурсами и данными.
2. Организация несанкционированного доступа к корпоративной сети.
3. Ограничение деятельности предприятия в определенной области.

Что именно может нести угрозу информационной безопасности любого предприятия:

- вредоносное программное обеспечение.
- мошенники-хакеры.
- инсайдеры-работники, действующие со злыми намерениями или по неосторожности.
- природные явления.

Чтобы реализовать угрозу есть несколько способов. Например, организовать перехват данных, оставить программную или аппаратную «закладку» или нарушить работу локальных беспроводных корпоративных сетей, организовать для инсайдеров доступ к инфраструктуре компании [6]. Так же стоит знать какие существуют системы защиты от утечек данных и чем они отличаются друг от друга, их я приведу в таблице №1. Каждый может выбирать ту систему, с которой ему будет удобнее работать, вы полностью не ограничены в выборе программ.

Вывод. Знание видов взлома и утечки данных информационных систем является неотъемлемой частью их защиты от уязвимости персональных данных.

Источники и литература

1) Баранова Е.К., Мальцева Л.Н. Анализ рисков информационной безопасности для малого и среднего бизнеса // Директор по безопасности. — 2015. — № 9. — С. 58—63.
2) Баранова Е.К. Методики анализа и оценки рисков информационной безопасности // Вестник Московского университета им. С.Ю. Витте. Серия 3: Образовательные ресурсы и технологии. – 2015. – № 1(9). – С. 73-79.
3) Баранова Е.К., Бабаш Л. В. Информационная безопасность и защита информации: Учеб, пособие. — 3-е изд., перераб. и доп. — М.: РИОР: ИНФРА-М, 2016. — 322 с. — (Высшее образование). — http://www.dx.doi.org/10.12737/1 1380
4) Сабанов А.Г. Многоуровневый анализ угроз безопасности процессов аутентификации //Вопросы защиты информации. – 2014. – № 1(104).
5) Баранова Е.К., Забродоцкий А.С. Процедура применения методологии анализа рисков OCTAVE в соответствии со стандартами серии ИСО/МЭК 27000-27005 // Вестник Московского университета им. С.Ю. Витте. Серия 3: Образовательные ресурсы и технологии. – 2015. – № 3(11). – С. 73-77.
6) https://itglobal.com/ru-ru/company/glossary/analiz-uyazvimostej/ [Дата обращения: 17.10.2022 в 19:07].
7) http://www.iee.unn.ru/wpcontent/uploads/sites/9/2018/02/2.Inf.ugrozy-vred.programmykomp.prestupleniya.pdf [Дата обращения: 17.10.2022 в 20:14].
8) https://www.securitylab.ru/news/534270.php [Дата обращения: 18.10.2022 в 20:47].
9) https://itsecforu.ru/2019/11/13/%F0%9F%95%B5%EF%B8%8F-8-%D0%BF%D0%BE%D0%BF%D1%83%D0%BB%D1%8F%D1%80%D0%BD%D1%8B%D1%85-%D0%BC%D0%B5%D1%82%D0%BE%D0%B4%D0%BE%D0%B2-%D0%B2%D0%B7%D0%BB%D0%BE%D0%BC%D0%B0-%D0%BE-%D0%BA%D0%BE%D1%82%D0%BE/ [Дата обращения: 22.10.2022 в 18:07].
10) https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q1/#id2 [Дата обращения: 22.10.2022 в 18:33].
11) https://searchinform.ru/informatsionnaya-bezopasnost/dlp-sistemy/kak-vybrat-dlp-sistemu/sravnenie-dlp-sistem/ [Дата обращения: 22.10.2022 в 19:17].
12) Актуальные киберугрозы: итоги 2021 года (ptsecurity.com) [Дата обращения: 23.10.2022 в 19:57].

Иллюстрации

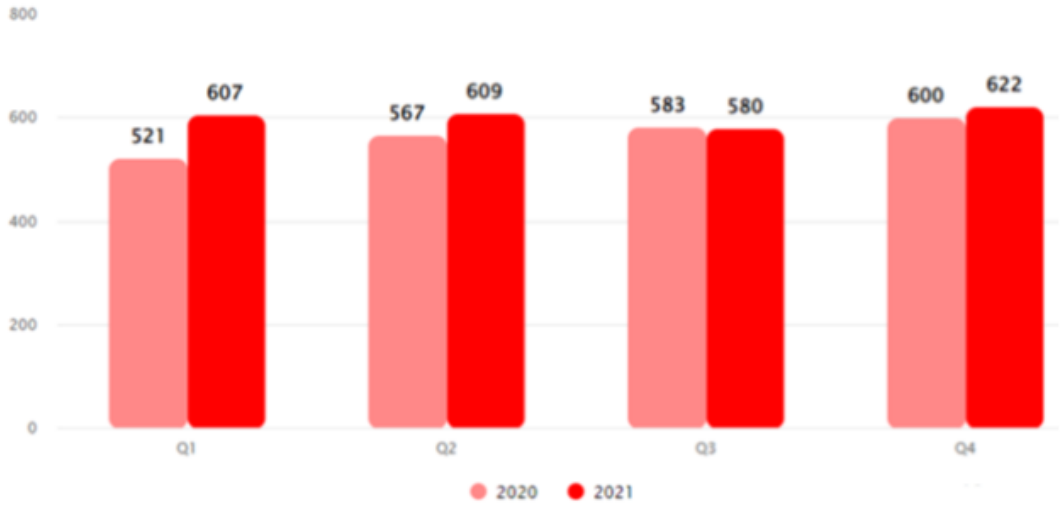

Рис. 1. Количество атак в 2020 и 2021 годах

Название DLP-системы	«Дозор-Джет»	Falcongaze	GTB Technologies	Infowatch	«МФИ Софт»	SearchInform	Symantec	Zecurion
Потребители	Крупная фирма, государственный сектор	Крупные компании, небольшие предприятия	Представители бизнеса независимо от сегмента	Услуги от ДЛП, например, СААС для фирмы независимо от величины	Бизнес среднего и крупного уровня	Крупные корпорации, сотрудники малого и среднего бизнеса	Мегакорпорация, в которой работают около 50-100 тысяч работников	Государственный сектор, крупная, средняя и маленькая компания
Расположение штаб-квартиры	Москва (РФ)	Москва (РФ)	Ньюпорт (США)	Москва (РФ)	Нижний Новгород (РФ)	Москва (РФ)	Маунтин Вью (США)	Москва (РФ)
Официальный сайт	dozor-jet.ru	falcongaze.ru	gtbtechnologies.com	infowatch.ru	mfisoft.ru	searchinform.ru	symantec.com	zecurion.ru
Предоставление услуг	Наличие технической поддержки, возможность пройти партнерское и клиентское обучение, услуги консалтинга и аутсорсинга	Техподдержка, помощь по внедрению, проведение обучения, а также оказание помощи по формировке информационной защиты в организации	Наличие техподдержки, обучение работников как в их центре, так и на рабочем месте	Услуги консалтинга в системе инфобезопасности	Возможность проведения удаленного обучения, оказание технической поддержки	Помощь по внедрению, техподдержка, обучение в учебном центре, аутсорсинг	Обучение персонала при помощи партнеров, внедрение	Проведение аудита, оказание консалтинговых услуг, оказание техподдержки, проведение обучения
Срок внедрения	До 7 календарных дней	От пары часов до нескольких дней. Все зависит от архитектурной сложности локальной сети компании	От одного до нескольких дней. Сроки зависят от масштабности внедрения и конфигурации корпоративной сети	От пары дней до семи рабочих дней. Зависит от того, насколько крупная фирма и какие задачи она решает	С того момента, как была получена заполненная анкета, нужно подождать семь дней, пока пройдет подготовка тех. решения, плюс двое суток, потраченных на установку	От одного раб. дня. Все зависит от предварительной подготовки и числа станций	От одних суток (учитывая масштаб внедрения)	Как и предыдущий
Язык панели управления	Только русский и английский (языки, которые входят в каждую систему)	Русский, английский, французский, испанский, итальянский, корейский, турецкий	Английский, польский, русский, китайский, немецкий, португальский	Украинский, международный английский, русский, белорусский	Исключительно русский	Русский, английский, латынь, польский, литовский	Английский, русский, японский, китайский, французский	Английский, русск

Рис. Таблица №1