ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ С УЧЕТОМ ЧЕЛОВЕЧЕСКОГО ФАКТОРА

Буркитбаев А.М.[1], Абеуов Р.Р.[2], Баширов А.В.[3]
Email: Burkitbayev17101@scientifictext.ru

[1]Буркитбаев Абылай Муратович – магистрант;
[2]Абеуов Роман Ринатович – магистрант;
[3]Баширов Александр Витальевич – кандидат технических наук, ведущий научный сотрудник,
кафедра информационно-вычислительных систем,
Научно-исследовательский институт экономических и правовых исследований
Карагандинский экономический университет Казпотребсоюза,
г. Караганда, Республика Казахстан

Аннотация: *обсуждаются аспекты: защита данных и информации, криптография и ее виды, а также методы атак на конфиденциальную информацию. Рассматриваются варианты атаки и защиты информации, в частности набирающий популярность метод социальной инженерии. Решаются часто встречаемые проблемы комплексной защиты информации. Обращается внимание на особенности человеческого фактора при защите данных. Авторы приходят к выводам о решении выбора комплекса защитных средств организации, составлении политики конфиденциальности на рабочем месте.*
Ключевые слова: *защита информации, криптозащита, методы взлома.*

PROBLEMS OF INFORMATION PROTECTION WITH THE ACCOUNT OF THE HUMAN FACTOR

Burkitbayev A.M.[1], Abeuov R.R.[2], Bashirov A.V.[3]

[1]Burkitbayev AbylayMuratovich – Graduate Student;
[2]Abeuov Roman Rinatovich – Graduate Student;
[3]Bashirov Alexander Vitalyevich – Candidate of Technical Sciences, Leading Researcher,
DEPARTMENT OF INFORMATION AND COMPUTING SYSTEMS,
KARAGANDA ECONOMIC UNIVERSITY OF KAZPOTREBSOUZ,
KARAGANDA, REPUBLIC OF KAZAKHSTAN

Abstract: *discussing aspects: protection of data and information, cryptography and its types and methods of attacks on confidential information. Discussing options for attack and protection of information, in particular the increasingly popular method of social engineering. Resolving frequent problems of complex information security. Attention is drawn to the peculiarities of the human factor in data protection. The authors come to conclusions about the solution selection of the complex of protective equipment, organization, drafting privacy policies in the workplace.*
Keywords: *protection of information, crypto protection, methods of hacking.*

УДК 004.056.53

С каждым днем количество информации увеличивается стремительными темпами, получить доступ к ней становится проще, чем до появления всемирной паутины - интернет. Но не каждому может быть дозволено ознакомиться с конфиденциальными данными. Именно для этого используется криптография. Криптография – наука, обозначившая свое присутствие в современном мире уже как необходимость.

В древние времена использовались простые методы перестановки и замены, но сейчас они неактуальны, так как слишком просты, и любой разбирающийся в принципах шифрования/дешифрования аналитик сумеет в кратчайшие сроки определить ключ для расшифровки сообщения. Самый простейший по сегодняшним меркам шифр Цезаря имеет ничтожную криптостойкость, и путем перебора ключа можно увидеть текст послания.

Благодаря развитию математики и компьютерной техники появилось огромное множество алгоритмов шифрования, которые из-за высокой криптостойкости позволили усложнить жизнь аналитикам. К настоящему моменту разработаны такие алгоритмы, как криптография с симметричным и ассиметричным (открытым) ключами, хэш-функции, а также цифровые подписи, сертификаты, VPN-туннели, RFID-метки, пароли и другие. Методы безопасности используются в разных сферах деятельности, от аптек, университетов, школ и супермаркетов, до банков и зданий государственных структур. Использование RFID меток в системах безопасности сейчас встречается практически везде, и все более новые устройства начинают поддерживать новые технологии, RFID датчики в телефонах, NFC, M1 для кодирования карточки в телефон, благодаря которой, также впоследствии можно использовать телефон для оплаты. Но чем больше новых устройств поддерживают новый функционал, тем больше

злоумышленники пытаются придумать способы взлома этих новшеств.

Но и аналитики, к коим можно причислить не только «хакеров», но и специалистов по информационной безопасности, не остаются в стороне и ищут новые способы для преодоления этих ограничения или проверки своей же системы защиты «на прочность». Если сам метод шифрования/дешифрования данных достаточно криптостойкий и сложный для взлома, то аналитик будет вынужден прибегнуть к другому способу получения необходимой ему информации. Так в статье Дэви Уиндера (DaveyWinder) выделяются 10 наиболее известных методов взлома. Расположены они в таком порядке эффективности:

1) атака по словарям,
2) брутфорс (BruteForce – с англ. грубая сила),
3) радужные таблицы (RainbowTables),
4) фишинг,
5) социальная инженерия,
6) вредоносное программное обеспечение,
7) оффлайн-хакинг,
8) банальное подглядывание через плечо,
9) шпионаж,
10) догадки [1].

В связи с перспективностью и эффективностью данных методов на 2017 год этот порядок можно изменить так:

1) социальная инженерия,
2) вредоносное программное обеспечение,
3) радужные таблицы.

Пункты подглядывание «через плечо», фишинг, шпионаж, догадки сейчас причисляются к социальной инженерии. Так как они являются частью логических размышлений криптоаналитика и попыток обойти защиту посредством самого слабого звена в системе – человека. Многочисленные исследования доказывают, что использование человеческого фактора может оказать фатальное и разрушительное действие на защиту системы.

Человек в силу своей природы не всегда задумывается о том, как защитить себя и свои данные от посторонних глаз. Он может безо всякого труда выдать свои идентификаторы, пин-коды, открыто работать с конфиденциальными данными, иметь очень простые пароли. Нетрудно представить последствия такой беспечности работника какой-либо организации.

Основной проблемой на сегодняшний день является не совсем полноценная защита данных. В большинстве статей описаны способы защиты данных в цифровом виде. Но мало где указывается аспект политики безопасности как необходимой меры [2].

С точки зрения информационной безопасности, тремя главными свойствами информации всегда являлись и являются доступность, целостность и конфиденциальность. При этом непосредственной задачей подразделения IT-службы являются прежде всего обеспечение бесперебойной доступности сервисов и обеспечение их корректной работы (целостности). Задача обеспечения конфиденциальности уже потребует полных знаний о содержимом данных и их ценности для этой организации. О полномочиях сотрудников по доступу к той или иной информации может судить лишь владелец – руководитель проекта, финансовый директор или другие. Иными словами тот, кто просто не обладает достаточными знаниями для принятия решений об обеспечении нужного уровня конфиденциальности в такой ситуации либо вводит общие ограничения, либо перекладывает решение о классификации контента на тех, кто способен реально оценить важность данных. Кроме этого, достаточно трудно внедрить защитные средства, что ограничат сотрудникам доступ, ведь основной задачей является как раз-таки обеспечить доступность.

Информационная безопасность в большинстве случаев понимается как обеспечение защиты не информационного контента и сотрудников организации, а самой IT-инфраструктуры.

Решением такого рода проблем будет комплексная защита данных, которая состоит в многоуровневой защите данных в IT-инфраструктуре и соблюдение конфиденциальности на уровне человеческого фактора [3].

Организация защиты IT-инфраструктуры у предприятия должна быть представлена не только антивирусными ПО, резервным копированием, устранением уязвимостей базового ПО, контролем доступа в сеть. Также должны применяться криптографические алгоритмы, цифровые подписи, сертификаты и многое другое.

Обращая внимание на особенности человеческого фактора, то тут защититься не так просто. Для защиты от атак социальной инженерии необходимым будет изучение разновидностей таких атак, понимание целей злоумышленников, не лишним будет оценка ущерба, который возможно будет причинен организации. На основе полученной информации можно будет интегрировать в политику

безопасности необходимые меры защиты.

Методы действия социальных инженеров:

- Представление при телефонном звонке другом/сотрудником/ партнером/представителем закона/руководителем/кем-либо еще с просьбой о помощи или приказом;
- Отправка вируса/кейлоггера/патча/фальшивых всплывающих окон и уведомлений по почте с целью удаленного получения информации, пользуясь доверием сотрудника;
- Физическое «подкидывание» зараженного носителя на территорию организации в ожидании, когда ничего не подозревающий сотрудник активирует вредоносное ПО;
- Модифицирование и подделка подписей/надписей/печатей посредством факса или e-mail для введения в заблуждение сотрудников.

Меры обеспечения безопасности при телефонном звонке предполагают скептическое отношение к любому виду просьб и проявлению «актерского» мастерства. Основные принципы: проверка личности звонящего, использование услуги АОН а также игнорирование sms-сообщений от неизвестных отправителей.

Мерами обеспечения безопасности при использовании электронной почты можно назвать конкретные принципы при работе с электронными письмами, содержащей вложения, гиперссылки, запросы на информацию как с территории организации, так и за ее пределами.

Таким образом, можно выделить следующие основные механизмы защиты для организаций:

- разработка продуманной политики классификации данных, которая учитывает те «безвредные» на первый взгляд данные, которые могут привести к утечке важной информации;
- обеспечение защиты клиентских данных с помощью шифрования или использования разграничений доступа;
- обучение всех сотрудников организации навыкам определения социальных инженеров;
- запрет на обмен паролями для персонала либо многократное использование одного общего на нескольких сотрудников;
- запрет на предоставление конфиденциальной информации из отделов кому-либо, не подтвержденному тем или иным способом;
- использование иных особых методов подтверждения личности для всех тех, кто запрашивал доступ к конфиденциальной информации;

В конечном итоге получаются несколько важных выводов.

Решение о выборе средств защиты информации организации должно приниматься не IT-службой, а руководителями, ответственными за безопасность бизнеса, с привлечением обладающих необходимой подготовкой специалистов в области защиты информации.

В классификации информации должны участвовать руководители подразделений, которые лучше других сотрудников понимают ценность создаваемой и обрабатываемой информации для организации и конкурентов, желающих ее заполучить.

Совместно со специалистами по защите информации разработать продуманную политику безопасности организации, включающую физическую защиту территории организации, ее внутренних сетей, контроль доступа и посещений, а также обучение персонала организации методам защиты от атак социальных инженеров.

Список литературы / References

1. Top ten password cracking techniques. [Электронныйресурс]. Режим доступа: http://www.alphr.com/features/371158/top-ten-password-cracking-techniques/ (дата обращения: 24.04.2017).
2. *Баширов А.В., Ханов Т.А., Сыздык Б.К., Оразметов Н.С.* Оценка риска информационной безопасности подразделения // Современные научные исследования и разработки,. 2016. № 6 (61). [Электронный ресурс]. Режим доступа: http://olimpiks.ru/zhurnal-sovremennyye-nauchnyye-issledovaniya-i-razrabotki/ (дата обращения: 23.04.2017).
3. Предотвратить НЕЛЬЗЯ поймать! [Электронный ресурс]. Режим доступа: http://www.ntks-it.ru/products/perimetrix/article1/ (дата обращения: 25.04.2017).