УДК 304,444

В. Г. Гарате
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)

Анализ уровня защищенности корпоративных компьютерных сетей в контексте социоинженерных атак

Представлена классификация социоинженерных атак, предложен возможный подход к оцениванию индекса защищенности корпоративных компьютерных сетей с точки зрения поведения человека. Рассматриваются способы защиты от атак социальной инженерии, и подчеркивается важность политики безопасности организации, а также обученности персонала.

Безопасность информации, вымогательство, социоинженерная атака, протокол, корпоративные компьютерные сети, кибер-атака

Тридцать пять лет тому назад, когда американская фирма IBM разработала первый персональный компьютер, не было речи об информационной безопасности. Персональный компьютер был создан для того, чтобы дать пользователю возможность выполнить свою личную работу. С последующим развитием сетей передачи данных и стандартизации стека протоколов TCP/IP развитие Интернета стало экспоненциальным.

После этого возникла необходимость разделения работы, работа в группах для совместного использования ресурсов и решения задач. Возникла потребность защиты информации каждого сотрудника и способов передачи ее в сетях определенной компании. В течение последних лет проблемы безопасности все в большей степени влияют на развитие и эксплуатацию сетей передачи данных (СПД) как в государственном и частном секторах, так и в мировом масштабе.

Важно определить разницу между безопасностью информации и информационной безопасностью. Под безопасностью информации понимается дисциплина, которая говорит о рисках, угрозах, анализе сценариев, передовой практике и схемах регулирования, а также требует уровней защищенности процессов и технологий для повышения уровня доверия к разработке, использованию, хранению, передаче, восстановлению и обеспечению доступности информации. Под информационной безопасностью понимается дисциплина, которая несет ответственность за проведение технических решений для защиты информации (активов), набор методов и техник, обеспечивающих защищенность информации («самых ценных ресурсов компании»).

Цель данной работы – оказать помощь администраторам компьютерной безопасности и другим специалистам в понимании важности компьютерной безопасности и обязанностей, которые она предполагает. Документ предусматривает обсуждение общих угроз безопасности, планирование и осуществление безопасной политики, а также контроль часто выполняемых мероприятий в области компьютерной безопасности [1]. В этом контексте безопасность информации имеет первостепенное значение, поскольку она помогает компаниям внедрять экономически эффективные меры безопасности.

В Перу и во всей Латинской Америке правительство и частные компании все чаще придают значение атакам социальной инженерии, они вкладывают время и деньги в подготовку работников, чтобы они поняли, что безопасность информации корпоративной сети является задачей всех работников в целом, а не только администраторов и высшего руководства.

Джон Дэвисон Рокфеллер (нефтяной магнат) написал в книге «Мой первый миллион»: «Окружите себя специалистами, платите своим работникам хорошо, создайте условия и оптимальную рабочую среду, и никогда не будет проблем в компании. На сегодняшний день это то, что компании не в состоянии понять».

Социальная инженерия. В течение длительного времени администраторы или компьютерные инженеры учились защищать свои корпоративные компьютерные сети от внешних атак (хакеров), теперь основная угроза исходит от сотрудников – от внутреннего нарушителя. Поведение человека, которое часто называют социальной инженерией, является одним из них. Согласно [2], социальная инженерия является искусством использования человеческого поведения для нарушения безопасности, когда участники (или жертвы) даже не подозревают, что ими манипулируют. Социальный инженер использует человеческие ошибки или уязвимости для того, чтобы получить доступ к корпоративным компьютерным системам и сетям, несмотря на меры безопасности, которые были реализованы в организации или отдельным человеком.

Есть две основные категории, в соответствии с которыми могут быть классифицированы все социоинженерные атаки, – обман на основе использования компьютера или компьютерной технологии и обман человека-оператора. Пользователь получает всплывающее окно, информирующее его о том, что в компьютерном приложении была проблема, и ему нужно будет повторно провести идентификацию и аутентификацию, чтобы продолжить. После того как пользователь вводит свой идентификатор и пароль на этом всплывающем окне, хакер, создавший всплывающее окно, получает идентификатор и пароль и осуществляет санкционированный доступ к корпоративной компьютерной системе и сети.

Человеческий подход реализуется посредством обмана, пользуясь невежеством жертвы и естественной склонностью человека быть полезным. Злоумышленник, подражая человеку с авторитетом, звонит службе поддержки и, делая вид, что он старший менеджер, говорит, что забыл свой пароль и должен получить его немедленно. Если ему предоставляют парольную информацию, злоумышленник может получить доступ к системам, как если бы он был менеджером, и может получить номера социального страхования и другую конфиденциальную частную информацию любого сотрудника [2].

Из интервью Кевина Митника, печально известного хакера 1980–90-х гг., с «BBC новости онлайн» [3]: «самой большой угрозой для безопасности предприятия является не компьютерный вирус, «дыра» в ключевой программе или плохо установленный брандмауэр. На самом деле, самой большой угрозой можете быть вы. Я лично пришел к выводу, что легче манипулировать людьми, чем технологией. Большинство организаций игнорируют человеческий фактор».

Для того чтобы обезопасить себя от воздействия социальной инженерии, необходимо понять как она работает. Рассмотрим основные типы социальной инженерии и методы защиты от них.

Один из видов интернет-атак – «всплывающее окно», поддельная программа злоумышленника, которая сообщает оператору, что связь приложения была прекращена из-за проблем в сети и теперь пользователь должен повторно ввести свой идентификатор и пароль для продолжения своей сессии. Ничего не подозревающий пользователь выполняет просьбу так быстро, как он может, потому что он хочет продолжить работу. Позже он узнает, что было совершено нападение на систему, но не понимает, что он был тем, кто открыл доступ. Как и троянский конь из греческой мифологии, злоумышленник может отправить безвредную, как представляется, электронную почту случайным получателям. Один из видов атаки состоит в том, что злоумышленник отправляет безвредное вложение электронной почты, которое ничего не подозревающая жертва открывает и таким образом запускает вирус или червь, который со временем может заразить всю сеть. Другой тип атаки – когда злоумышленник обещает вознаграждение, если получатель направит его к определенному числу людей. Это может быть привлекательно, и получатель часто впадает в искушение сделать то, что было предложено. А результатом является экспоненциальная нагрузка на сетевые ресурсы, что может остановить работу сети.

«Dumpster дайвинг» является техникой, служащей для получения информации, которая может быть использована для проведения атаки на компьютерную сеть. Телефонные книги компаний

и организационные диаграммы предоставляют телефонные номера и адреса сотрудников, особенно сотрудников управленческого звена, которые могут работать на злоумышленника. Процедуры и правила могут помочь хакеру получить данные о политике и процедурах компании и, таким образом, убедить жертву в их подлинности. Календари являются важными источниками информации о встречах, отдыхе и т. д. Хакер может использовать их для улучшения своей «сюжетной линии», когда он хочет обмануть ничего не подозревающего секретаря компании.

Злоумышленник может использовать лист бумаги с печатным бланком компании, чтобы создать необходимую официальную переписку. Нарушитель может получить конфиденциальную информацию с жесткого диска компьютера. Есть способы получения информации с дисков, даже если пользователь считает, что данные были «удалены» с диска. Для предотвращения dumpster дайвинга компании должны установить политику по отходам, где все бумаги, распечатки или носители информации стираются, и весь персонал должен быть извещен об опасности неотслеживаемого мусора.

Доступ к информации можно получить, представившись сотрудником службы технической поддержки и запросив пользователя о получении доступа к его рабочей станции с целью «исправить» некую техническую проблему. Ничего не подозревающий пользователь, особенно если он не является технически грамотным, вероятно, даже не задает никаких вопросов или не смотрит, что делает с его компьютером так называемый технический специалист [4]. Здесь пользователь пытается быть полезным и исполнить свою роль в попытке решить проблему в сети компании.

Сколько людей будет подозревать уборщика помещения в возможности взломать сеть? Человек, одетый как уборщик, входит в рабочую зону, неся оборудование для очистки. В процессе уборки вашей зоны работы он может шпионить и получить ценную информацию, например пароли или секретные файлы, которые вы забыли закрыть, или может сделать телефонный звонок с вашего стола, выдавая себя за вас. Или возьмем случай ложного телефонного ремонтника. Злоумышленник может возиться вокруг вас с инструментами, проводами с целью шпионить и получать ценную информацию.

Злоумышленник может вызвать компьютерную справочную службу компании и пожаловаться на проблемы с доступом к системе [2]. Он будет утверждать, что очень спешит, и немедленно нуждается в сбросе пароля, требуя дать пароль по телефону, а персонал технической службы делает то, что просят.

Обучение и политика аудита. Успех любого предприятия зависит от квалифицированной, этичной и хорошо информированной рабочей силы. В первую очередь, требуется убедить руководство пригласить специалистов в области информационной безопасности, во-вторых, разработать и проводить информационно-просветительские программы, необходимые для того, чтобы привить информационную безопасность как добавленную стоимость к рабочей силе. Везде, где это возможно, безопасность информации должна быть встроена в бизнес-процессы. Для достижения этой цели безопасность информации должна быть в целом признана и принята в качестве отдельной ценности в рамках институциональной культуры, которая влияет на поведение работника [5]. Безопасность информации не может полагаться исключительно на технические или физические элементы управления. Сотрудники должны быть надежными, чтобы бизнес работал должным образом.

Как социализированные люди мы верим тому, что нам говорят, и оказываем помощь, когда ее просят. В частности, на работе, где соблюдаются правила общественной иерархии, мы должны действовать с определенной долей профессионализма. Очевидно, что без эффективной программы осведомленности об информационной безопасности информация организации находится под угрозой.

Сущностью хорошей политики безопасности информации является обучение, которое должно быть обязательным для всех сотрудников (от самых простых до самых важных работников) во всех организациях без исключения. Чтобы политика была эффективной, образование должно быть обычным явлением в организации. Некоторые компании требуют, чтобы все сотрудники пересматривали политику каждый год, чтобы ознакомиться с изменениями, если таковые имелись. Все новые сотрудники и неслужащие должны быть обучены, как только они начинают работу в компании [6].

Существует необходимость проводить аудит и мониторинг соблюдения политики безопасности информации по всему предприятию. Процедуры аудита должны проверить, например, чтобы человек, осуществляющий техническую поддержку, не отправлял пароли по телефону или через электронную почту в незашифрованном виде. Менеджеры

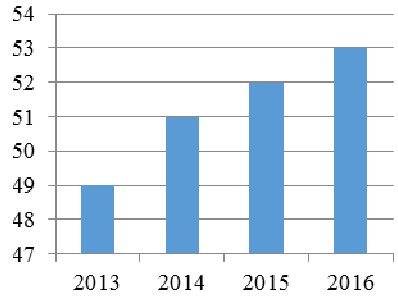

Рис. 1

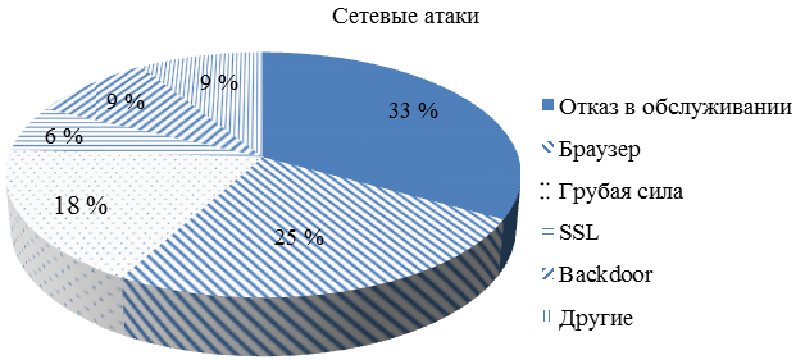

Рис. 2

периодически должны пересматривать доступ своих сотрудников. Аудит безопасности должен подтвердить, что сотрудники, которым больше не нужен доступ к сети, не будут иметь доступа к информации компании.

Меры по снижению воздействия антропогенных факторов, влияющих на информацию, следующие:

– хорошо документированная и доступная политика безопасности;

– обучение выполнению положений политики безопасности;

– осознание угрозы и влияние социальной инженерии в организации;

– внедрение и аудит использования политики;

– политика управления идентификацией;

– операционные процедуры для ограничения уязвимостей;

– использование физических технических решений (интеллектуальных вращающихся дверей), биометрических систем для устранения или уменьшения несанкционированного физического доступа;

– смягчение затрат со страховой защитой.

На рис. 1 (процент атак социальной инженерии в год) и рис. 2 (процент каждого типа атаки) приведены статистические данные по текущему состоянию дел в области атак на информацию на основе социальной инженерии.

Организация может уменьшить влияние атак социальной инженерии внедрив комплексную стратегию информационной безопасности. Такая стратегия должна включать меры по осведомленности в вопросах безопасности и образовательные программы, постоянное обучение, аудит и частый мониторинг всех событий в корпоративных сетях.

СПИСОК ЛИТЕРАТУРЫ

1. Best Practices for Enterprise Security. URL: https://msdn.microsoft.com/es-es/cc750076.

2. Protection du personnel interne contre les menaces d'ingénierie sociale. URL: https://technet.microsoft.com/fr-fr/library/cc875841.aspx.

3. How to hack people. URL: http://news.bbc.co.uk/2/hi/technology/2320121.stm.

4. Social Engineering your employees to Information Security. URL: https://www.sans.org/.../engineering/social-engineering-employee.

5. Compendio de Normatividad sobre el uso de TI en el Perú. URL: http://www.ongei.gob.pe/publica/metodologias/5125.pdf.

6. Big Data: vers l'ingénierie sociale? URL: http://www.internetactu.net/2014/05/20/big-data-vers-lingenierie-sociale.

W. G. Garate

Saint Petersburg Electrotechnical University«LETI»

ANALYSIS OF SECURITY LEVEL OF CORPORATE NETWORKS IN THE CONTEXT OF SOCIO-ENGINEERING ATTACKS

The paper states the classification of socio-engineering attacks, suggests a possible approach to the evaluation of security index of corporate computer networks from the point of view of human behavior. This work describes social engineering and its threat to the organization, it addresses the various forms of social engineering, and how they take advantage of human behavior. It also considers the security methods against social engineering attacks, and emphasizes the importance of the organization's security policy, as well as staff training.

Information security, ransomware, socio-engineering attack, protocol, corporate computer networks, cyber-attack