Гельфанд А.М., Кузнецов С.А., Анучин К.Н. Совершенствование защиты от социальных атак в области информационной безопасности// Международный журнал информационных технологий и энергоэффективности. – 2024. –
Т. 9 № 4(42) с. 89–94

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056

СОВЕРШЕНСТВОВАНИЕ ЗАЩИТЫ ОТ СОЦИАЛЬНЫХ АТАК В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

[1]Гельфанд А.М., [2]Кузнецов С.А., [3]Анучин К.Н.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: [1]amgelfand@mail.ru, [2]Killingsprin@bk.ru, [3]anucin221@gmail.com

Статья посвящена анализу роли человеческого фактора в информационной безопасности и методам противодействия атакам социальной инженерии. В условиях возрастающей численности и сложности кибератак основное внимание авторов сосредоточено на изучении влияния человеческого фактора и способах его минимизации как ключевого элемента в защите информации. Анализируются различные формы социальной инженерии и подходы к обучению персонала с целью повышения осведомленности о методах кибермошенников. Авторы делают акцент на необходимости разработки комплексного, ориентированного на человека подхода к информационной безопасности, который включал бы не только технологические решения, но и меры по увеличению осведомленности и подготовленности пользователей и персонала.

Ключевые слова: Информационная безопасность, социальная инженерия, кибератаки, противодействие мошенничеству.

IMPROVING PROTECTION AGAINST SOCIAL ATTACKS IN THE FIELD OF INFORMATION SECURITY

[1]Gelfand A. M., [2]**Kuznetsov S. A.**, [3]**Anuchin K. N.**
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: [1]amgelfand@mail.ru, [2]Killingsprin@bk.ru, [3]anucin221@gmail.com

The article is devoted to the analysis of the role of the human factor in information security and methods of countering social engineering attacks. In the context of the increasing number and complexity of cyber attacks, the main attention of the authors is focused on studying the influence of the human factor and ways to minimize it as a key element in information protection. Various forms of social engineering and approaches to personnel training are analyzed in order to increase awareness of the methods of cyber fraudsters. The authors emphasize the need to develop a comprehensive, human-centered approach to information security that would include not only technological solutions, but also measures to increase the awareness and preparedness of users and staff.

Keywords: Information security, social engineering, cyber attacks, fraud mitigation.

Введение

Информационная безопасность является одной из основных причин беспокойства для многих компаний. С ростом числа кибератак и их обескураживающей изощренностью задача защиты информации стала еще более сложной. Хотя при обсуждении нарушений безопасности в средствах массовой информации преобладают технологические сбои, львиную долю которых занимают вредоносные программы и использование уязвимостей программного обеспечения, становится все более очевидным, что человеческий фактор может сыграть значительную роль в подрыве усилий организации по обеспечению безопасности. В данной статье мы попытаемся рассмотреть с теоретической точки зрения, как можно решить проблему человеческого фактора в безопасности. Основное внимание будет уделено социальной инженерии - атакам, которые основаны на взаимодействии с человеком для получения конфиденциальной информации. Эти атаки могут иметь различные формы и осуществляться в любой точке цепочки - от первоначальной разведки цели до попытки создания черного хода. Хочется надеяться, что благодаря расширению исследований в этой области и разработке теорий о том, как можно снизить эти риски, удастся сместить акцент с исключительно технологических решений по защите от информационных рисков и перейти к более значимой роли таких аспектов, как осведомленность и развитый, ориентированный на человека, многоуровневый подход к обеспечению информационной безопасности. В этом вступлении мы попытаемся дать краткую характеристику отчета в целом и затронуть некоторые ключевые моменты, которые будут обсуждаться далее [2,4].

1. Понимание атак социальной инженерии

Атаки с использованием социальной инженерии часто являются первым шагом на пути к более крупному и сложному вторжению в организационные системы. Социальная инженерия - это получение информации от людей, обычно той, которая должна быть секретной. Большинство пользователей компьютеров и мобильных устройств знают об угрозе безопасности, которую представляют вирусы и другие вредоносные программы, даже если они не очень хорошо разбираются в этих угрозах. В результате многие пользователи принимают меры по защите от этих угроз. Однако многие пользователи еще не знают о потенциальных рисках, связанных с социальной инженерией. В отличие от вредоносных программ, о которых часто предупреждают, угрозы социальной инженерии обычно не пытаются проникнуть в компьютер или мобильное устройство пользователя. Вместо этого тактика социальной инженерии часто используется для того, чтобы обманом заставить пользователя предоставить доступ или информацию, которая может быть использована для получения доступа к организационным системам. В последние годы сочетание большего количества атак, больших потенциальных выплат и все еще относительно низкой осведомленности пользователей об опасности социальной инженерии сделало эти виды атак все более популярными среди киберпреступников. В немалой степени это связано и с тем, что использование социальной инженерии для взлома систем обычно требует от злоумышленников наименьших усилий и ресурсов по сравнению с более техническими атаками. Многие люди еще не усвоили первый урок защиты от кибератак, который заключается в том, что каждый должен играть важную роль в обеспечении безопасности систем. Это особенно верно в отношении социальной инженерии; хотя обучение и подготовка пользователей очень важны, не только от них зависит, будут ли они распознавать и

предотвращать атаки. Организации также могут помочь защитить себя и своих сотрудников, используя соответствующие технологии и устанавливая эффективные физические барьеры безопасности. Однако, безусловно, без тщательного обучения пользователей и программ подготовки даже самые надежные технологии и решения безопасности могут быть легко обойдены теми, кто использует методы социальной инженерии для проникновения в систему организации. Поэтому в статье не только предлагаются различные решения в виде методов обучения пользователей и технологических средств защиты от социальной инженерии, но и в заключении говорится о крайне важности наличия соответствующего режима, направленного на оценку и постоянное совершенствование средств защиты для удовлетворения потребностей постоянно меняющихся угроз социальной инженерии [1, 4].

2. Повышение осведомленности и обучение пользователей

Как уже говорилось в предыдущих разделах, эффективными методами противодействия социальной инженерии являются программы обучения пользователей и повышения их осведомленности о безопасности. Пользователи часто являются самым слабым звеном в системе безопасности организации, просто потому, что злоумышленнику необходимо манипулировать ими для достижения своих целей. Обычно сотрудники имеют определенный уровень доступа к сетям и системам организации, и их восприимчивость к атакам - человеческая уязвимость - часто используется злоумышленниками в своих интересах. Поэтому проактивный подход к снижению рисков социальной инженерии заключается в формировании и поддержании у пользователей мышления, ориентированного на безопасность, а также в обучении их распознаванию атак социальной инженерии и защите от них. Это включает в себя понимание тактики социальных инженеров - например, предотвращение человеческой склонности доверять безоговорочно или распознавание различных форм обмана - и создание сообщества пользователей, в котором существует коллективная ответственность за безопасность, что часто называют "обороной вглубь". Это включает в себя не только повышение уровня осведомленности человека о безопасности во время работы, но и усиление его бдительности на всех этапах повседневной жизни, где он взаимодействует с информационными технологиями. Ведь социальная инженерия не только атакует информационные системы организаций, но и представляет собой серьезную угрозу личной конфиденциальности в киберсреде. Включение тематического контента по защите частной жизни в материалы по безопасности также может помочь расширить понимание людьми конфиденциальности на различных онлайн-платформах и в приложениях. Конечной целью программы повышения осведомленности и обучения пользователей является создание культуры безопасности в организации: культуры, которая будет поддерживаться и проявляться на протяжении многих лет при постоянной поддержке как сотрудников, так и высшего руководства. В следующем разделе я расскажу о последних инициативах и практиках, направленных на вовлечение сотрудников в деятельность по повышению осведомленности о безопасности и дальнейшее создание устойчивой культуры безопасности, ориентированной на пользователей [5].

3. Внедрение технических средств контроля

Как отмечает Янг в книге "Кибербезопасность для индустрии 4.0", постоянно меняющийся ландшафт киберугроз означает, что злоумышленники постоянно пытаются найти новые векторы атак. Именно поэтому так важны расширенные функции, которые предлагают межсетевые экраны нового поколения. Предоставляя разнообразные методы защиты сети с акцентом на выявление различных потенциальных атак и защиту от них, можно свести к минимуму шансы стать жертвой атаки нулевого дня.

Один из способов, с помощью которого злоумышленники постоянно пытаются обмануть защиту, - это использование уязвимостей "нулевого дня". Это недостатки в программном, аппаратном или микропрограммном обеспечении, которые еще не известны разработчикам и производителям. В результате отсутствуют патчи и исправления, а значит, злоумышленники могут использовать эти уязвимости в ущерб технологическим пользователям.

Современные решения в области кибербезопасности движутся в сторону внедрения более совершенных межсетевых экранов, таких как брандмауэры нового поколения. Такие брандмауэры часто включают в себя дополнительные функции поверх стандартных технологий, такие как глубокая проверка пакетов, защита и обнаружение вторжений, проверка на уровне приложений. Благодаря этим функциям, а также функциям блокировки и ограничения скорости для различных правил брандмауэра, они могут обеспечить более сложную защиту от социальной инженерии, поскольку весь спектр методов атак, используемых злоумышленниками, постоянно меняется и развивается [3.4].

Брандмауэр - важнейшая часть кибербезопасности. Он действует как барьер между доверенной и недоверенной сетью и контролирует трафик, разрешенный к передаче в сеть и из нее. В настоящее время большинство крупных организаций и корпораций используют ту или иную технологию брандмауэра. Однако не все брандмауэры построены одинаково. Некоторые организации могут выбрать брандмауэр, который использует только предопределенные правила для разрешения или блокирования трафика - такие брандмауэры называются статическими брандмауэрами с пакетной фильтрацией. Другие могут использовать динамическую фильтрацию пакетов, когда брандмауэр проверяет экземпляр соединения на предмет его валидности и затем создает динамическое правило, позволяющее пропускать дальнейший трафик. Аналогично, брандмауэры с проверкой состояния работают на транспортном уровне модели OSI и отслеживают состояние активных соединений. Это означает, что если соединение было установлено доверенным лицом, дальнейший трафик в течение сессии будет разрешен [2,5].

И IDS, и IPS могут обнаруживать целый ряд различных атак, но наиболее эффективны против конкретных типов атак. Например, сетевые IDS и IPS лучше всего выявляют угрозы, исходящие из Интернета или других сетевых устройств.

Существует множество различных типов технологий, которые при правильном применении повышают эффективность защиты от социальной инженерии. К ним относятся системы обнаружения вторжений (IDS), системы предотвращения вторжений (IPS) и межсетевые экраны. IDS - это пассивная система, которая способна обнаруживать возможные атаки, нарушения безопасности, а также отслеживать и вести журнал потенциальной вредоносной активности. IPS - это активная система, которая при обнаружении угрозы предпринимает заранее определенные действия. Например, она может отправить предупреждение системному администратору или закрыть порт.

В мире современных технологий каждый день создаются новые вредоносные программы и схемы социальной инженерии, которые используются злоумышленниками. Поэтому очень важно следить за современными технологиями и обеспечивать адекватную защиту от этих атак [3].

4. Оценка и совершенствование защиты

Теперь масштаб вашего проекта очевиден. Вы знаете, какие технологии используются в вашей среде, и осведомлены о потенциальных векторах атак с помощью социальной инженерии. Поэтому вам необходимо оценить, насколько хорошо данная технология способна предотвращать и обнаруживать социальные атаки. Как всегда, совершенствование технологий может оказаться непосильной задачей, однако изменения и улучшения можно начать с простых вещей. Необходимо регулярно устанавливать исправления и обновления по мере их появления. Многие производители выпускают патчи сразу после выхода своего продукта, потому что в нем есть определенная уязвимость. Когда патч выпущен, хакер может воспользоваться уязвимостью, поэтому важно поддерживать системы в актуальном состоянии по мере появления таких патчей. Также убедитесь, что технология имеет обновленные списки потенциально вредоносных сайтов и известных фишинговых сайтов, чтобы сотрудники не попали на них по ошибке. В большинстве случаев поставщики продуктов регулярно предоставляют обновления этих списков, поэтому важно следить за тем, чтобы технология обновлялась. Это особенно полезно при защите от программ-вымогателей, поскольку криптографические методы вымогателей меняются. Поскольку технология находится на стадии оценки, важно понимать, что плохие результаты не всегда связаны с неэффективностью технологии. Проблема может заключаться в том, что текущая технология не позволяет решить всю проблему, технология развернута неправильно или, возможно, не подходит для защиты организации. Вот почему важно начинать пересмотр и изменение технологии с мелочей, с изменений, которые можно внести без масштабных последствий, и с изменений, которые можно достаточно легко реализовать. Это может быть что угодно - от внедрения новой технологии безопасности до такой простой вещи, как более строгие политики паролей. Эффективность изменений можно регулярно проверять, проводя учения "красной команды", и предпочтительные исправления и улучшения должны быть основаны на результатах этих учений.

Список литературы

1. Белопахов А.С. Использование игры «CAPTURE THE FLAG» как инструмента формирования навыка отражения кибератак у профессиональных программистов//Вестник науки. – 2023. – Т. 3. – №. 5 (62). – С. 584-589.
2. Беляцкий Н.П., Подупейко А.А. Цифровая трансформация: время меняться. – 2020.
3. Гасанов З.З., Вардидзе Р.Т. Обеспечение безопасности JAVA-приложений//Неделя науки-2021. – 2021. – С. 66-67.
4. Понин Ф.Н. Трансформация области COMPUTER SCIENCE под влиянием новейших технологических инноваций//Universum: технические науки. – 2023. – №. 12-1 (117). – С. 59-64.

5. Shestakova L., Akhmetzyanov R. The use of E-learning elements by a mathematics teacher in work with schoolchildren //Mathematics at school. – 2023. – T. 3. – №. 116. – C. 35-44.

References

1. Belopakhov A.S. Using the game "CAPTURE THE FLAG" as a tool for developing the skill of repelling cyber attacks among professional programmers //Bulletin of Science. – 2023. – T. 3. – №. 5 (62). – pp. 584-589.
2. Byalyatsky N.P., Podupeiko A.A. Digital transformation: time to change. – 2020.
3. Hasanov Z.Z., Vardidze R.T. Ensuring the security of JAVA applications //Science Week-2021. – 2021. – pp. 66-67.
4. Ponin F.N. Transformation of the field of computer science under the influence of the latest technological innovations //Universum: technical sciences. – 2023. – №. 12-1 (117). – pp. 59-64.
5. Shestakova L., Akhmetzyanov R. The use of E-learning elements by a mathematics teacher in work with schoolchildren//Mathematics at school. – 2023. – Vol. 3. – No. 116. – pp. 35-44.