МЕТОДОЛОГИЧЕСКИЙ ПОДХОД К ПРОГРАММЕ ПОВЫШЕНИЯ ОСВЕДОМЛЕННОСТИ О БЕЗОПАСНОСТИ

Бозаров Фарход Самадович

Старший преподаватель, Университет экономики и педагогики

Негосударственное образовательное учреждение

Annotation: *В настоящее время люди в сочетании с социально-техническим аспектом могут быть либо самым сильным, либо самым слабым звеном в любой информационной безопасности, и ключ к безопасности заключается в проведении обучения по повышению осведомленности с помощью коротких и эффективных онлайн-видео, с помощью которых участник может получить знания о безопасности. Поэтому наша цель состоит в том, чтобы разработать инновационные решения для предоставления интерактивной программы повышения осведомленности о кибербезопасности, основной целью которой является расширение информации об осведомленности и знаниях в области безопасности в организациях, школах, странах, домах и т. д. Программа, которую мы представляем, состоит из уникального системный подход, разделенный на три целевые группы: основные, предварительные и управленческие. Также мы представляем другой метод измерения знаний каждого участника и сравниваем его с базовым опросом, проведенным во время регистрации.*

Ключевые слова: *кибербезопасность, осведомленность, учебный план, человеческий фактор, социально технический, безопасность.*

METHODOLOGICAL APPROACH TO SECURITY AWARENESS PROGRAM

Bozarov Farkhod Samadovich

The senior teacher of University of Economics and Pedagogy Non-governmental educational institution, Uzbekistan

Abstract: *Currently, humans coupled with the socio-technical aspect can be either the strongest or the weakest link in any information security, and the key in security lies in delivering awareness training through short and effective online videos, whereby the participator can gain knowledge on security. Our aim, therefore, is to develop innovative solutions to deliver an interactive cybersecurity awareness program, where the main goal is to enhance information on security awareness and knowledge in organizations, schools, nations, homes etc. The syllabus that we present consists of a unique systematic approach divided into three target groups: basic, advance and management. Also we present a different method in measuring the knowledge of each participant, and compare it to the base-line survey carried out during the registration. Our results show the participant's awareness level of knowledge. By implementing this program in private and public organizations, governments, schools and universities will lead to the improvement of IT security awareness levels in the everyday use of computers, mobile phones, online banking, and social networking - both at home and in the workplace.*

Keywords: *cybersecurity, awareness, socio-technical, human factor, syllabus, security;*

В настоящее время предприятия, организации и граждане считают информационно-компьютерные технологии (ИКТ) бесценными для выполнения повседневных задач, как дома, так и на рабочем месте. По аналогии с большей частью населения, организации и предприятия могут страдать от нарушений безопасности. Это связано с уязвимостями новых и существующих технологий, а также конвергенцией устройств. Такие нарушения безопасности могут быть связаны с ИТ или могут быть результатом инцидентов, вызванных человеческим фактором. Недавние истории показали, что значительное число конечных пользователей не знают о своей подверженности риску безопасности. Из-за недавних нарушений безопасности как никогда важно, чтобы организации повышали осведомленность о безопасности, превращая пользователей в первую линию обороны. [1]

Осознание – это не тренировка. Цель информационных презентаций – просто привлечь внимание к безопасности. Презентации для повышения осведомленности предназначены для того, чтобы люди могли распознавать проблемы с безопасностью ИТ и реагировать соответствующим образом. [2]

Таким образом, в этой статье в следующем исследовании представлены результаты, опубликованные в книге, и главная цель состоит в том, чтобы охватить осведомленность на национальном уровне о самом слабом элементе безопасности, предоставив учебный план. Программа касается различных целевых групп и определяет концепцию коммуникаций. Кроме того, он определяет цели и задачи программы. Следовательно, он определяет показатель для измерения успеха программы и фокусируется на предоставлении «передовой практики». Механизмы оценки и обратной связи являются важнейшими компонентами любой программы повышения осведомленности о безопасности. Таким образом, базовые исследования текущего состояния проводятся заранее и направлены на отслеживание преимуществ, приносимых программой повышения осведомленности. Для получения обратной связи от респондентов использовались оценочные анкеты. [4]

В соответствии с этими целями мы обобщаем наш основной подход и методологию с помощью представленных результатов, чтобы решить и повысить уровень осведомленности и знаний за счет положительных результатов в результате реализации учебной программы в школах, университетах, частных и общественных организациях.

Текущий уровень осведомленности. Основное внимание в исследовании уделяется в первую очередь изучению ответа на предшествующую озабоченность по поводу безопасности и уровня знаний для защиты информационных активов, а также предложению уже реализованных подходов для повышения уровня осведомленности. Опрос проводился среди 1000 участников отовсюду, в возрасте от 11 до 63 лет, в различных профессиях, таких как школы, университеты, частные и общественные организации.

Текущий уровень осведомленности. Основное внимание в исследовании уделяется в первую очередь изучению ответа на предшествующую озабоченность по поводу безопасности и уровня знаний для защиты информационных активов, а также предложению уже реализованных подходов для повышения уровня осведомленности. Опрос проводился среди 1000 участников отовсюду, в возрасте от 11 до 63 лет, в различных профессиях, таких как школы, университеты, частные и общественные организации.

Кроме того, многие организации, школы и страны применяют различные подходы для повышения уровня осведомленности о безопасности. Кроме того, предоставила информационные материалы по безопасности и разработала информационный сайт по вопросам безопасности, на котором размещены информационные презентации, видеоролики и плакаты. Дополнительные примеры выделены в разделе «Обсуждение».

Однако существуют огромные различия между каждой программой повышения осведомленности. До сих пор почти все академические усилия в обучении информационной безопасности были сосредоточены на решении технических и политических аспектов проблемы, а не на разработке систем и механизмов безопасности с учетом человеческого фактора. Таким образом, человеческий фактор является наиболее уязвимой угрозой в системе. Где, в конце концов, это ставит под угрозу общую эффективность организации и нации.

Тем не менее, новые предложения могут превосходить фактический стиль реализации программ повышения осведомленности о безопасности, и разделяет его идеи о том, что цель состоит в том, чтобы изменить понимание людьми рисков и, в конечном итоге, изменить их поведение. Ключом к программе повышения осведомленности, которая создает безопасную среду, является ответ на следующие три вопроса: Кто? - определяет цель вашей программы повышения осведомленности; Что? - определяет содержание того, что донести и научить людей; Как? - это средства, с помощью которых вы передаете

контент. Также многие из существующих программ повышения осведомленности устарели и используют традиционные методы обучения, такие как: презентации, тренинги и т.д. [5]

По этой причине мы создали новый подход и методологию, которые определяют ответы на три вышеуказанных вопроса. Целевыми группами программ повышения осведомленности являются: базовая, предварительная и управленческая. Мы определяем содержание того, что доставлять и учить. Дополнительно общение осуществляется посредством коротких онлайн-видео – не более 10 минут. И, наконец, проводится базовый опрос для измерения уровня информированности каждого участника заранее.

Силлабус - Программа предлагает новый системный подход для разных групп: базовая, продвинутая и управленческая. Каждая часть содержит определенное количество модулей, разделенных на блоки, которые изучаются в отдельной главе/учебной программе.

Учебный план построен на том, что мы должны делать и что необходимо сделать, чтобы информационная безопасность была безопасной, либо избегая, либо смягчая инциденты безопасности. В целом, идея программы состоит в том, чтобы помочь, улучшить и повысить уровень осведомленности трех различных типов групп информационной безопасности. Подчеркнем, что самым слабым элементом является человеческое поведение, за которым следует социально-технический аспект. Однако эта программа не охватывает правовые аспекты, связанные с вопросами информационной безопасности.

Для того, чтобы программа была интригующей, после каждого блока мы снабдили викторинами-анкетами, где участники должны были дать ответ. После отправки ответа изменить запись невозможно. Поэтому участник может ответить на вопросы только один раз. Однако, чтобы иметь возможность дать правильный ответ в нижней части каждого блока, мы представили новый подход с дополнительными материалами для чтения и подсказками, которые помогут и направят участника заранее получить наиболее разумный ответ на

вопросы. Также после завершения процесса регистрации участники перенаправляются на базовый опрос, основная идея которого заключается в том, чтобы заранее измерить знания, а затем изучить и отметить сходство или различие полученных знаний.

Цели учебной программы состоят в том, чтобы успешно предоставить решения для наилучшей практики использования технологий. Затем следует, как защитить личную, а также информацию организаций. Кроме того, знать и знать, как настроить беспроводные сети для личной выгоды и, в конечном итоге, как понять, что вы стали жертвой онлайн-мошенничества, и, наконец, интерпретировать фильтрацию спама. Учебная программа разделена на три типа подходов к обеспечению безопасности, таких как: физическая безопасность, компьютерная и мобильная безопасность; и безопасность сети и Интернета. Во-первых, подход физической безопасности показывает очень эффективные методы защиты вашего персонального компьютера и рабочей станции, защиты мобильных и портативных устройств, за которыми следуют чрезвычайно важные вопросы безопасной печати. Кроме того, подход к обеспечению безопасности компьютеров и мобильных устройств касается вредоносного программного обеспечения, безопасности операционной системы и способов создания надежных и безопасных паролей. Наконец, модуль сетевой и интернет-безопасности выполняет эффективную манипуляцию и обман людей, такие как социальная инженерия и социальные сети, которые важны для повседневного безопасного просмотра.

Предоставляются решения о том, как идентифицировать фишинг и выполнять успешный онлайн-банкинг, а также идентифицировать раздражающий спам по электронной почте и сообщениями мгновенных сообщений, а затем использовать брандмауэр и безопасность беспроводной сети при регулярной работе.

Число конечных пользователей компьютеров растет как на дрожжах. Их контроль над компьютерами также увеличивается. Учебники, учебные,

экспериментальные и обучающие среды доступны бесплатно, и они позволяют конечным пользователям технологии разработать комплексное программное обеспечение и получить полный контроль или функциональность программного обеспечения, сети, тестирования, анализа, разработки и т. д. Хотя совершенствование технологий и Интернета соответствует повседневным требованиям, обязательствам и производительности продвинутых пользователей, существует множество способов обойти защиту. В этом вопросе, если пользователи являются опытными или профессиональными компьютерами, они осознают, что могут стать жертвами или подвергнуться риску. Поэтому чрезвычайно важно и желательно, чтобы деятельность по повышению осведомленности принималась во внимание, определяя, что опытные пользователи или, другими словами, специалисты по компьютерам на самом деле являются теми, кто может выполнять и выполнять такие действия, как настройка сети, программирование, устранение неполадок, установка и т.д.

Тем не менее, эта учебная программа представляет собой общую анатомию атаки и таксономию инструментов, используемых в этом процессе; он предоставляет буквальные сценарии хакерских действий и решения для защиты от атак. В целом он представляет собой разумную тактическую модель процесса наброска и построения атаки, дополненную техническим обзором инструментов, использованием шагов, используемых в этом процессе, и, наконец, решением. Общая структура атак на стандарты компьютерных систем обычно описывается в таких подходах, как и, где они помогают создать структуру, тогда как, с другой стороны, мы предпочитаем учебную программу, а не разделить целевую фазу атаки на следующие компоненты: разведка, сканирование, получение доступа, поддержание и расширение доступа, заметание следов и сокрытие. [6]

Управление информационной безопасностью - это структурированный процесс внедрения и постоянного управления информационной безопасностью в организации. Он включает действия, направленные на защиту информации и

информационных объектов для обеспечения непрерывности бизнеса. Поэтому важно, чтобы управление информационной безопасностью рассматривалось как любая жизненно важная бизнес-функция, и все его действия основывались на бизнес-потребностях. Тем не менее, все менеджеры являются пользователями, но с другой стороны все пользователи не являются менеджерами. В третьем и последнем курсе этой программы повышения осведомленности мы фокусируем и раскрываем проблемы, которые могут возникнуть в организации, предназначенной для управленческого персонала. [7] На самом деле, мы подчеркиваем важность понимания процесса принятия решений, особенно в наши дни, когда управленческий персонал в любой организации имеет дело и должен находить ответы на повседневные инциденты, возникающие из-за информационной безопасности. Тем не менее, в этом курсе по менеджменту мы отмечаем этапы процесса принятия решений, подробно описывая циклы PDCA (ISO, 2009) и OODA, куда мы также включили оптимизацию затрат и осведомленность о кибербезопасности. [8]

В целом большой процент участников выходит в Интернет с помощью различных типов широкополосных коммуникационных технологий, типичным для которых является использование компьютера. Кроме того, озабоченность по поводу безопасности своих активов информационных технологий, таких как компьютер и ноутбук, периферийные устройства, электронные данные и мобильные устройства, выровнена и варьируется от чрезвычайной до наименее обеспокоенной. Точно так же диапазон по шкале от чрезвычайно осведомленных до наименее осведомленных о защите своих активов информационных технологий очень разнообразен. Кроме того, самые большие угрозы их информационным технологиям связаны с систематическим подходом к наиболее известным угрозам. Таким образом, местная защита, используемая для их компьютерных и электронных данных, является согласованной. Кроме того, участники считают, что вирусы, черви, хакеры и злоумышленники являются самыми серьезными угрозами, а вредоносное программное

обеспечение, спам и другие нежелательные электронные письма считаются гораздо менее значительными. Кроме того, участники защищают свой персональный компьютер или электронные данные с помощью антивирусного программного обеспечения, которое регулярно обновляется, а также брандмауэра.

Например, физическая безопасность, которая составляет 60%, затем для компьютерной и мобильной безопасности средний балл, набранный пользователями во внутренних подразделениях, составляет 64%, и, наконец, для модуля сетевой и интернет-безопасности средний балл, набранный пользователями, составляет 70%, что также является наивысшим показателем. В модуле физической защиты мобильное и портативное устройство безопасности имеет самый высокий балл, в частности блок защищенной печати, имеет самый низкий балл. Где в компьютерном и мобильном модуле безопасности блоки вредоносного ПО и надежных и безопасных паролей находятся практически на одном уровне со средним процентным баллом, отличающимся от блока безопасности операционной системы. А в последнем модуле «Безопасность сети и Интернета» самый высокий средний процентный балл был получен в блоке «Безопасный просмотр»:

- Физическая безопасность 59,71%;
- Защитите свой компьютер 52,86%;
- Защита данных 65,09%;
- Мобильная и портативная безопасность 67,24%;
- Безопасная печать 48,67%;
- Компьютерная и мобильная безопасность 63,96%;
- Вредоносное ПО 67,50%;
- Безопасность ОС 61,96%;
- Надежный и безопасный пароль 66,05%;
- Безопасность сети и Интернета 70,30%;
- Социальная инженерия и сети 65,38%;

- Безопасный просмотр 85,71%;
- Безопасность электронной почты и обмена мгновенными сообщениями 57,14%;
- Брандмауэр 67,14%;
- Безопасность беспроводной сети 68,57%;

Настоящие результаты предлагают несколько направлений действий, чтобы решить и повысить уровень знаний с положительными результатами. Результаты на данный момент были очень обнадеживающими, и они подтвердили, что метод и подход нашей интерактивной программы повышения осведомленности о кибербезопасности являются решающими и непобедимыми. Внедрение программы улучшит повседневную работу и использование компьютеров, мобильных телефонов, онлайн-банкинга и социальных сетей, а также поможет определить необходимые действия в будущем.

В целом, по отзывам участников, они нашли темы и разделы интересными. Хотя многие учащиеся имели достаточно хорошие теоретические знания об угрозах, связанных с ИТ-активами, они считали полезным практиковать теорию и наиболее известные практики. Даже человек, более компетентный в компьютерной и мобильной безопасности, чем мы, сказал, что смог научиться новым трюкам и что викторины были увлекательными. Еще одна отмеченная деталь заключалась в том, что, хотя вы можете часто читать о новых уязвимостях или проблемах безопасности, у вас обычно просто не хватает мотивации или времени, чтобы вникать в практическую безопасность. В заключение мы находим, что выбор тем достаточно эффективен, хотя можно рассмотреть возможность дальнейшего улучшения. Естественно, нам необходимо постоянно обновлять список тем и искать новые интересные идеи.

Угрозы кибербезопасности постоянно развиваются. Таким образом, мы должны обеспечить, чтобы не только специалисты, защищающие ИТ-системы, получали надлежащее информационное образование, но и простые, обычные пользователи и менеджеры. Таким образом, только существенные изменения в

восприятии, культуре и образовании пользователей могут эффективно снизить количество нарушений информационной и кибербезопасности. Следовательно, это повысит уровень осознания человеческого фактора при использовании технологий и в повседневной жизни.

Используемая литература:

1. European Network and Information Security Agency - ENISA (2010), A users guide: How to raise information security awareness, Nov 29.
2. Mark Wilson and Joan Hash (2003), Building an Information Technology Security Awareness and Training Program, Computer Security, NIST Special Publication 800-50, October.
3. Lance Spitzner (2010), How to build an effective information security awareness program, October.
4. Predrag Tasevski (2013), Interactive Cyber Security Awareness Program, LAP LAMBERT Academic Publishing, Aug 10
5. Lance Spitzner (2010), How to build an effective information security awareness program, October.
6. Susan Young and Dave Aitel (2003), The Hackers Handbook: The Strategy behind Breaking into and Defending Networks, Auerbach Publications, Nov 24.
7. Clive Vermeulen and Rossouw Von Solms (2002), The information security management toolbox – taking the pain out of security management, Information Management & Computer Security, Vol. 10 Iss: 3, pp.119 - 125.
8. H.A. Kruger, W.D. Kearney (2006), A prototype for assessing information security awareness, Feb.