Донецкий Национальный Технический Университет

Лабораторная работа № 1

«Угрозы и задачи»

Выполнил:

ст. группы ИПЗ -13

Лысенко А. С.

Проверила:

доцент каф. ПМИ

Маслова Н. О.

Покровск 2017

Вариант 9

Служба безопасности предприятия выявила ряд угроз информационной безопасности предприятия. Классифицируйте представленные угрозы по основным критериям классификации угроз (по аспекту ИБ, по компонентам ИС, по способу осуществления, по расположению источника) и предложите меры по их ликвидации.

|  |  |
| --- | --- |
|  | **Описание угрозы** |
| 1 | Злоумышленники закрепили на здании устройство считывания и мониторят информацию, передаваемой по сетям в незашифрованном виде, в том числе собирают статистику о времени передачи информации, протоколах, объемах передаваемых данных, IP-адресах респондентов и т.п. |
| 2 | «Обиженный» системный администратор сознательно игнорирует выполнение своих обязанностей, нарушает регламент проведения антивирусных проверок, не своевременно предоставляет права доступа «вредным» пользователям, некорректно ведет себя при необходимости смены паролей пользователя (издевки, отсутствие предупреждений), предлагает приятелям мастер-классы по настройкам сервера |
| 3 | При проведения текущего ремонта в комнате, имеющей общие коммуникации с комнатой, где размещено серверное оборудование, системный администратор отдал ключи прорабу для выполнения ремонтных работ в любое удобное тому время. |

Ответ оформите в виде таблицы вида:

1)

|  |  |  |  |
| --- | --- | --- | --- |
| № | Угрозы | Агент/среда реализации угрозы | Предложения по способам предотвращения угрозы |
| 3 | Анализ трафика | Угрозы, связанные с получением злоумышленником паролей и иной информации (в том числе конфиденциальной), передаваемой по сетям в незашифрованном виде, а также сбором статистической информации о времени передачи информации, используемых протоколах, приложениях участвующих в обмене данными, частоте, объемах и характере передаваемых данных которые в дальнейшем могут быть использованы для проведения атаки | Использовать алгоритмы шифрования, для передачи информации по сети. Оцепить здание охраняемой территорией |
| № | Угрозы | Агент/среда реализации угрозы | Предложения по способам предотвращения угрозы |
| 13 | Вредоносная атака -манипулирование ИТ-оборудованием | Угрозы, варьирующиеся от несанкционированного ознакомления с конфиденциальной информацией до уничтожения носителей данных или систем. Могут осуществляться как внешними, так и внутренними нарушителями по различным причинам (корыстными целями, мести или в результате нервного срыва) | Использовать алгоритмы шифрования, для передачи информации по сети. Оцепить здание охраняемой территорией |
| 16 | Вредоносные программные средства | Угрозы потери конфиденциальности, целостности информации, нарушения нормального функционирования системы в результате воздействия вредоносного программного обеспечения |  |
| 30 | Кража данных/документов | Угрозы, связанные с потерей конфиденциальности, потерей данных (в случае отсутствия резервной копии) или утерей важных документов (в том числе и доказательных) |  |
| 33 | Нарушение законодательства | Угрозы нарушения законодательства вследствие использования слишком слабых алгоритмов для шифрования данных (например, персональных данных), требований к хранению архивных данных (минимальных периодов хранения документов, требований по защите информации, требований по использованию цифровой подписи) |  |
| 35 | Небрежное обращение с данными | Угроза потери конфиденциальности и целостности информации вследствие небрежного обращение с данными, например допуска подглядывания и подслушивания, оставление мобильного оборудования и носителей данных без присмотра и т.д. |  |
| 38 | Разглашение документов/данных | Угроза разглашения конфиденциальных документов/ данных в результате недостатка контрольных мер, действий злоумышленников, преднамеренных или непреднамеренных действий или бездействий персонала |  |
| 39 | Разглашение/ раскрытие пароля | Угрозы раскрытия паролей из-за легкости их подбора, подглядывания, записывания на бумажках или в незашифрованных файлах, перехвата их во время передачи по сети в незашифрованном виде, что может привести к получению несанкционированного доступа как внешнему, так и внутреннему нарушителю |  |
| 46 | Неконтролируемое копирование документов | Угроза потери конфиденциальности вследствие несанкционированного копирования документов (особенно при их транспортировке, отправке почтой или помещении в архив) |  |
| 79 | Прослушивание линий | Угрозы разглашения конфиденциальной информации, особенно при использовании беспроводной связи и протоколов без шифрования данных. |  |
| 86 | Утрата конфиденциальности | Угрозы потери конфиденциальности информации находящейся на внутренних носителях данных (жестких дисках), внешних носителей данных, распечатанных копий, передаваемой по телекоммуникационным линиям в результате случайного или преднамеренного несанкционированного чтения, копирования, чтения с резервных копий, кражи носителей информации, мониторинг каналов передачи данных, чтение данных с экрана монитора. Чем секретнее информация, тем больше усилий будут прилагать третьи стороны, чтобы получить ее |  |

2)

|  |  |  |  |
| --- | --- | --- | --- |
| № | Угрозы | Агент/среда реализации угрозы | Предложения по способам предотвращения угрозы |
| 12 | Вредоносная атака -манипулирование данными или программным обеспечением | Угрозы, связанные с вводом неверных данных, изменениях в правах доступа, в бухгалтерских данных, переписке, операционных системах или программного обеспечения, с различными целями, в том числе и с разрушительными (например, мести) | Установить сотрудника на должность по наблюдению за действиями системного администратора, в обязанности которого будет входить обход пользователей системного администратора и сбора нерешенных проблем |
| 16 | Вредоносные программные средства | Угрозы потери конфиденциальности, целостности информации, нарушения нормального функционирования системы в результате воздействия вредоносного программного обеспечения |  |
| 18 | Затруднительное отыскание неисправностей | Угрозы, связанные с затруднительным отысканием неисправностей, что может привести к позднему обнаружению неисправности, либо увеличить необходимое время на восстановление |  |
| 20 | Злоупотребление администраторскими правами | Угрозы, преднамеренного нанесения ущерба системе или пользователям, связанные со злоупотреблениями прав администратора (в том числе полученными злоумышленником). Следует иметь в виду, что в Unix системах нет ограничений прав пользователя root |  |
| 24 | Использование программного обеспечения несанкционированным образом | Угроза преднамеренного несанкционированного манипулирования программным обеспечением или данными в системах баз данных авторизованными пользователями в различных целях |  |
| 26 | Использование известных уязвимостей | Угрозы распространения вирусов, отказа в обслуживании или получения несанкционированного доступа к ресурсам вследствие использования известных уязвимостей программного обеспечения или операционных систем |  |
| 36 | Потеря доступа авторизованными пользователями | Угрозы потери целостности или отказа в обслуживании вследствие внезапной потери доступа авторизованными пользователями |  |
| 41 | Неисправность/ выход из строя программного обеспечения | Угрозы потери целостности или отказа в обслуживании вследствие сбоев или отказа программного обеспечения |  |
| 60 | Не использование патчей (программных коррекций) программного обеспечения для исправления известных уязвимостей безопасности | Угрозы, связанные с действиями вредоносного программного обеспечения или сбоев программного обеспечения в результате не использования программных коррекций для используемого программного обеспечения |  |
| 89 | Файловые вирусы | Угрозы, порчи информации, отказа в обслуживании, в результате заражения файловыми вирусами (которые распространяются путем прикрепления к открываемым на зараженной системе файлам, и заражают систему при открытии такого файла) |  |

3)

|  |  |  |  |
| --- | --- | --- | --- |
| № | Угрозы | Агент/среда реализации угрозы | Предложения по способам предотвращения угрозы |
| 31 | Кража оборудования | Угрозы, связанные с потерей конфиденциальности, потерей данных (в случае отсутствия резервной копии) или недоступности, вдобавок к непосредственным затратам на приобретение замены украденного ИТ оборудования | Назначение сотрудника для слежение за проведение ремонтных работ, проведение инструктажа по ответственности персонала |
| 42 | Неисправность электропитания | Прямые угрозы, непосредственно влияющие на ИТ технику и системы. Косвенные связанные с отключение систем, чья работоспособность влияет на ИТ технику и системы (например, сбой ИБП, который после короткого перебоя электропитания по каким-то причинам не смог автоматически переключиться в штатный режим работы, что может привести к разряду батареи и отключению питаемой им системы) |  |
| 54 | Несанкционированный доступ к комнате | Угрозы конфиденциальности, целостности или доступности связанные с предоставлением прав доступа к комнатам некомпетентным или ненадежным сотрудникам, злоупотреблениями ими или несанкционированным получением доступа нарушителем |  |
| 62 | Ошибка рабочего персонала | Угроза, связанная с незнаниями или недостаточным знанием существующих правил и процедур, приводящие к тому что сотрудники не знают, за что они ответственны и как им необходимо реагировать на штатные и нештатные ситуации, или вследствие нарушения внимания у персонала, находящегося в неблагоприятных рабочих условиях (рабочее место организованно с нарушениями требований эргономики, мешает громкий шум, плохое освещение и т.д.) |  |
| 66 | Перепады напряжения/ перенапряжения/ флуктуации | Широкий спектр угроз от небольших инцидентов, не несущих большого вредоносного эффекта на ИТ системы (включая компьютерные и телефонные сети) до полного выхода их из строя, вследствие огромных скачков напряжения |  |
| 70 | Выход из строя источника бесперебойного питания (ИБП) | Угрозы, связанные с неспособностью ИБП выполнять свои функции вследствие неисправности |  |
| 71 | Повреждение коммуникационных сервисов | Угроза отказа коммуникационных сервисов вследствие аварий, сбоев программно-аппаратных средств, действия вредоносного ПО, ошибок персонала и т.д. |  |
| 82 | Случайный ущерб, авария по вине персонала или из за поломки оборудования | Угрозы, связанные с ущербом в результате аварий произошедших вследствие поломки оборудования или ошибочных действий персонала |  |
| 90 | Электростатический заряд | Угроза выхода из строя оборудования в результате электростатического заряда |  |