
НИКИТА ШАХУЛОВ
ЭТИЧНЫЙ
ХАКЕР
КИБЕРБЕЗОПАСНОСТЬ

Никита Шахулов
Этичный хакер

http://www.litres.ru/pages/biblio_book/?art=67618266
ISBN 9785005640161

Аннотация

Этичный хакер (пентестер) – это специалист в сфере кибербезопасности, который профессионально занимается выискиванием «дыр» в коде и помогает устранить утечки данных. Название специальности происходит от англоязычного термина pentest (penetration test), то есть «тест на проникновение». Имеется в виду проникновение в систему через скрытые уязвимости.

Содержание

Этичный хакер

Никита Шахулов

ISBN 978-5-0056-4016-1
Создано в интеллектуальной издательской системе Ridero

Изучение этического взлома может стать катастрофой, если вы пренебрегаете этими 7 правилами

Нападение на собственные системы самообороны для проверки уязвимостей считалось главной военной стратегией еще 1500 лет назад.

Атака на собственные системы для проверки устойчивости к атакам, возможно, помогла многим нашим предкам выиграть войны, укрепив их слабые места. Тенденция продолжается и по сей день во имя «этического взлома», когда уязвимости в киберсистемах вынюхиваются, а системы укрепляются против атак.

Новый вид битвы ведется на нас в этот день, не на поле боя, а в цифровом мире. Киберпреступность-самая быстрорастущая область преступности, и никто не находится в безопасности. Интернет принес много анонимности своим пользователям, и хакеры и киберпреступники используют эту анонимность для совершения преступлений. Этический взлом был создан из-за необходимости активно противостоять киберугрозам и улучшать защиту для защиты интересов уязвимых сторон.

Этический взлом сегодня это большой бизнес. Google, Facebook («Организация, запрещенная на территории Рос-

сийской Федерации»), Twitter и другие крупные компании тратят миллионы на «взлом белой шляпы», чтобы вынюхивать уязвимости в своих системах. Программы Bug bounty, где хакеры будут получать компенсацию за сообщения об уязвимостях, станут нормой в будущем. Организации доверяют людям, которые были сертифицированы как этические хакеры, поскольку они знают кодекс поведения, которому следует следовать во время курсов по этическому хакерству. Но даже самый искренний этический хакер может споткнуться и попасть в ситуации, которые могут нанести вред хакеру или организации. Даже сертифицированные этические хакеры должны понимать некоторые правила, прежде чем практиковать взлом белой шляпы.

• Вы хакер в белой шляпе, но вам все равно нужно разрешение, прежде чем взламывать систему пользователя:

взлом белой шляпы может быть этичным, но взлом системы пользователя без явного разрешения от них приведет к неприятностям. На самом деле взлом, даже в этических целях без явного разрешения владельцев, является уголовным преступлением в большинстве стран.

• Понять бизнес и организационную структуру вашего клиента: прежде чем начать заниматься этическим взломом, важно понять бизнес и систему вашей клиентской организации. Это даст вам представление о чувствительности их сети и о том, как вам нужно обрабатывать любую конфиденциальную информацию, с которой вы можете столкнуться.

• Не превышайте лимиты, налагаемые клиентом: даже если ваш клиент предоставил вам полный доступ к своей сети, все равно может быть предел тому, сколько вы можете копать. Не копайте глубже, чем вам сказали, так как вы можете нарушить доверие клиентов.

• Убедитесь, что вы выполняете свою работу правильно, чтобы не поставить под угрозу защитные системы клиента: ваша задача-вынюхивать дыры и следить за тем, чтобы эти дыры были исправлены для укрепления системы ИТ-безопасности. Предоставьте подробный отчет о своих выводах и убедитесь, что вы не переступаете никаких ограничений или не нарушаете никаких законов или правил. Планируйте, прежде чем выполнять тесты этического взлома, поскольку время и терпение имеют первостепенное значение для чувствительных результатов.

• Будьте прозрачны со своими клиентами: открытое общение с вашим клиентом поможет не только вашему клиенту, но и вам, повысив вашу надежность. Вы должны раскрыть все открытия, которые вы сделали, своему клиенту, чтобы он мог принять необходимые меры предосторожности для защиты своих систем. Ваш клиент должен быть в курсе того, что происходит в любое время.

• Будьте конфиденциальны и этичны: вы должны сохранять конфиденциальность вовремя и даже после выполнения работы. Вы этичный хакер, и трудовая этика для вас на первом месте, и это включает конфиденциальность кли-

ента. Раскрытие секретов ваших клиентов третьим лицам уничтожит саму цель этического взлома. Поддерживайте ценности и цели компании и уважайте их конфиденциальность.

• Заметайте следы: вы проникли в системы и предложили подробные очистки. Но при выходе вы должны убедиться, что не оставляете следов и тем самым защищаете систему от будущих атак.

Этический взлом-чувствительная и иногда опасная работа. Но каждый этический хакер должен следовать заповедям этического взлома, поскольку существует очень тонкая грань между черной шляпой и белой шляпой. Оставайтесь сосредоточенными и верными себе, и вы добьетесь успеха

4 Ключевые особенности COBIT 5 Foundation для улучшения карьеры

COBIT означает" Цели контроля за информацией и связанными с ней технологиями. Он был запущен профессиональной ассоциацией ISACA, которая расшифровывается как Ассоциация аудита и контроля информационных систем, в качестве основы надлежащей практики. Мотивом создания COBIT было создание простейшей и общей среды для взаимодействия между различными бизнес-личностями.

Первая версия COBIT была выпущена в 1996 году. Затем в 1998 году была разработана версия 2, а в 2000 году она была расширена до версии 3. Версии 4 и 4.1 были запущены последовательно в 2005 и 2007 годах соответственно. Последняя версия COBIT 5 была выпущена в апреле 2012 года.

COBIT был создан для управления и управления информационными технологиями. COBIT предназначен для внедрения ИТ – практик (управления и управления) в организации. Можно отслеживать и, таким образом, улучшать действия, направленные на достижение целей. Таким образом, он имеет целую руку на требованиях к контролю и технических вопросах.

Хорошо обоснованные организации понимают

цель COBIT. Он помогает в предоставлении моделей управления ИТ, что также помогает в предоставлении данных из ИТ и проверке данных для измерения и управления рисками и другими факторами.

После версии COBIT 4.1 мы достигли COBIT 5, которая является последней версией глобальной платформы ISACA. Эта версия COBIT предоставляет бизнес-руководителю практики, модели и различные инструменты, которые помогут повысить эффективность и точность значений, полученных от информационных систем.

4 Ключевые особенности COBIT 5

1. Первая важная особенность COBIT 5 заключается в том, что она была выпущена с эволюцией от модели зрелости COBIT 4.1 до модели технологических возможностей COBIT 5. Обе модели выполняют одну и ту же задачу, но структура фреймворка в новой модели возможностей процесса изменена.

2. COBIT 5 дает функцию сбалансированной системы показателей (BSC), которая используется для понимания бизнес-ценностей ИТ. Он используется в различных организациях для измерения выполнения предприятия в различных областях.

3. COBIT 5 создан, чтобы уделять больше внимания бизнесу и ИТ как интегрированной форме. Это поможет улучшить систему организации, поскольку уточнение ролей и коммуникаций и предотвращение ущерба предприятию от некоторых проблем, связанных с информацией и технологиями.

4. COBIT 5 разработан, чтобы уделять больше внимания цели процесса, добавляя больше ценности подходу, используемому здесь, по сравнению с COBIT 4.1.

Это сделало COBIT 5 совершенно новой концепцией по сравнению с предыдущей версией, хотя она по-прежнему выполняла ту же задачу.

COBIT 5 был построен на некоторых основных, но важных принципах. ISACA сама подняла эти принципы, которые:

- **Удовлетворение потребностей заинтересованных сторон**
- **Охват предприятия от начала до конца**
- **Применение единой интегрированной структуры**
- **Обеспечение целостного подхода**
- **Отделение управления от управления**

Подводя итог, разработка COBIT показала совершенно новый способ управления системой для руководителя бизнеса. Это, будучи основой надлежащей практики, сделало управление и управление простыми, как никогда раньше.

Важность PCI; стандарт безопасности данных (DSS)

По мере того, как мир движется к цифровым платежным средствам и транзакциям, также возникают опасения по поводу безопасности и защиты информации о держателях карт. По данным Совета по стандартам безопасности PCI, с 2005 года было взломано более 500 миллионов записей владельцев карт с конфиденциальной информацией.

Торговцы, которые принимают цифровые формы платежей, находятся в центре цифровых платежей и могут стать жертвой финансового мошенничества в нескольких точках, включая:

- Устройство или машина для продажи
- Беспроводные точки доступа
- Подключенный компьютер или любое другое устройство
- Передача данных держателя карты поставщику услуг.

Факторы риска

Согласно бизнес-опросу, проведенному Forrester Consulting, большинство предприятий проводят мероприятия, повышающие риск мошенничества с картами, включая хранение номера карты, срока годности, любого проверочного кода и даты клиента.

Введение в стандарт безопасности данных (DSS)

Стандарт безопасности данных индустрии платежных карт (PCI-DSS) является стандартом безопасности, обязательным для организаций, которые обрабатывают платежи с использованием карт, выпущенных основными типами карт, включая MasterCard, Visa и American Express.

Этот стандарт PCI является обязательным для всех марок карт и управляется Советом по стандартам безопасности PCI. Единственной целью стандартов PCI является защита данных держателей карт и снижение мошенничества с картами.

Цели

Целью PCI-DSS является защита данных держателей карт при хранении, обработке и передаче. Информация о владельце карты включает уникальный номер основного счета (PAN), напечатанный на лицевой стороне каждой карты.

Торговцы или любой поставщик услуг, которые обрабатывают платежи по картам, никогда не должны хранить конфиденциальную информацию о транзакции после авторизации. Это включает в себя конфиденциальные данные, которые хранятся в магнитной полосе карты, а также любую личную идентификационную информацию, введенную держателем карты.

Требования

Стандарты безопасности данных PCI определяют список из 12 обязательных требований, которые сгруппированы по 6 целям контроля, как указано ниже:

1) Построение и обслуживание сети высокого уровня безопасности, которая включает в себя:

*** Установка защищенного брандмауэра для защиты данных держателей карт.**

Это ограничивает (или блокирует) весь трафик из ненадежных сетей и запрещает прямой публичный доступ между Интернетом и средой данных держателя карты.

*** Изменение пароля по умолчанию, предоставленного поставщиком, и других мер безопасности.**

Это важно, так как большинство мошенников с картами могут проникнуть во внутреннюю сеть владельца карты, используя пароли по умолчанию.

2) Защита информации о держателях карт, которая включает в себя:

*** Шифрование информации о держателях карт, которая передается по общедоступным сетям.**

Технология шифрования делает передаваемые данные нечитаемыми любым посторонним лицом. Для защиты данных клиентов можно использовать криптографию и протоколы безопасности, такие как SSL/TLS или IPSec.

*** Защита сохраненных данных держателей карт.**

Конфиденциальные данные на магнитном чипе карты не должны храниться. В случае, если PAN необходимо сохранить, он должен храниться в нечитаемом формате. Ограничьте продолжительность хранения данных о держателях карт.

3) Сопровождение программы управления уязвимостями, которая включает в себя:

*** Использование и регулярное обновление антивирусных программ на всех системах.**

Вредоносные вирусы могут проникать в сеть пользователя через электронную почту и другие онлайн-действия. Антивирусное программное обеспечение является эффективным инструментом для защиты компьютерных систем от внешних атак.

*** Разработка и сопровождение защищенных систем и приложений.**

Уязвимости безопасности в системе и приложениях могут позволить киберпреступникам получить доступ к PAN и другим защищенным данным. Убедитесь, что все системы и приложения обновлены последним патчем безопасности от поставщика.

4) Меры безопасного контроля доступа, которые включают в себя:

*** Ограничение доступа бизнеса к информации о держателях карт.**

Ограничьте доступ к конфиденциальным данным держателей карт только тем пользователям, работа которых требует этой информации. Кроме того, ограничьте доступ к наименьшему количеству данных, необходимых для бизнес – целей.

*** Присвоение уникального идентификатора каждому человеку с доступом к компьютеру.**

Это важно, чтобы иметь возможность отслеживать, был ли доступ к критическим данным выполнен только уполномоченными лицами.

5). Ограничение физического доступа к данным держателей карт.

Физический доступ к данным держателей карт должен быть ограничен всем персоналом, посетителями и всеми бумажными и электронными носителями.

6) Регулярный мониторинг и тестирование сетей, которое включает в себя:

*** Отслеживание и мониторинг всех точек доступа к сетевым ресурсам и данным держателей карт.**

Использование механизмов ведения журнала и отслеживания действий пользователя включены.

*** Регулярное тестирование процедур и процессов безопасности.**

Периодическое тестирование средств контроля безопасности важно наряду с внутренним и внешним сканированием сети.

7) Ведение политики информационной безопасности, которая включает:

*** Поддержание политики компании, направленной на обеспечение информационной безопасности.**

Это включает в себя создание политики безопасности, которая учитывает все требования PCI-DSS, а также ежегодный процесс обнаружения любой уязвимости.

Этот набор требований является обязательным для компаний, производящих устройства, которые принимают и обрабатывают транзакции на основе PIN-кода или любой другой тип цифровых платежей.

Финансовые учреждения, продавцы и поставщики услуг должны гарантировать, что они используют только устройства, одобренные для PTS (PIN transaction security).

Важность ИТ-безопасности в онлайн-бизнесе

Нет ракетостроения в понимании того, почему ИТ-безопасность важна для вашего бизнеса. Прошли те дни, когда люди писали тысячи документов, чтобы защитить свои ценные данные. Это цифровой мир, и мы все зависим от технических устройств, которые мы несем, куда бы мы ни пошли. Эти важные и конфиденциальные данные могут сделать или сломать ваш бизнес, поэтому он всегда остается уязвимым в некоторой степени, и всегда были разные опасения по поводу его безопасности. Нет сомнений в том, что компании стараются изо всех сил защитить свои данные, однако есть и другие силы, которые постоянно пытаются сломать вашу безопасность и украсть ваши данные. Именно поэтому важно поддерживать ваши данные в курсе современных технологий, чтобы защитить их от кражи.

Ниже приведены некоторые статистические данные и моменты, которые помогут вам понять, почему каждый владелец бизнеса должен держать свою ИТ-безопасность императивом над чем-либо еще.

Аналогичный риск для крупного и малого бизнеса:

Как упоминалось в отчете, опубликованном департаментом кибербезопасности правительства в 2016 году, 65% крупных фирм обнаружили нарушение кибербезопасности или любую кибератаку в прошлом году. 25% тех же компаний также отметили, что сталкиваются с этими нарушениями хотя бы раз в месяц. В целом эти нарушения стоили крупным фирмам более 3 миллиардов фунтов стерлингов, а в среднем эти нарушения стоили 36 500 фунтов стерлингов.

Не только крупные фирмы, малые предприятия или стартапы также были целью киберпреступников. Существует множество причин, по которым малые предприятия становятся мишенями киберпреступников. Обычно малые предприятия не концентрируются на своей ИТ-безопасности из-за различных причин, таких как нехватка ресурсов и человеческих сил. Вот почему они являются легкими целями, но не такими прибыльными, как крупные фирмы для киберпреступников. Недавно накопленные данные о нарушениях кибербезопасности на малых и средних предприятиях обошлись им в прошлом году в 310 800 фунтов стерлингов. Эти цифры не столь значительны по сравнению с потерей владельцев крупного бизнеса, но скорость, с которой он подско-

чил в этом году с 2014 года, вызывает тревогу. Общая стоимость в 2014 году составила всего 115 000 фунтов стерлингов, что почти удвоилось всего за один год.

Фирмы должны быть готовы к большему количеству атак, чем когда-либо в этом году

Учитывая темпы роста этих кибератак за последние два года, ожидается, что в этом году будет больше атак, чем когда-либо. Одной из причин такого резкого увеличения числа атак являются стартапы и новые предприятия, которые недооценивают свою ИТ-безопасность и больше заботятся о создании своего бизнеса в первую очередь. С каждым годом предприятия, которые полностью зависят от компьютеров и Интернета, теряют больше, чем зарабатывают. Эти фирмы не идут в ногу с каждым новым обновлением безопасности. И наоборот, киберпреступники оснащают себя всеми новейшими технологиями и становятся все более смертоносными с каждым годом.

Нет никаких сомнений в том, что эти малые предприятия являются излюбленными целями киберпреступников. Более того, эти малые предприятия также стали причиной беспокойства для крупных фирм. Многие крупные фирмы нанимают небольшие компании в качестве своих поставщиков, которые выполняют для них различную работу. Киберпреступники используют эту связь больших и малых фирм и нарушают сильные системы крупных фирм, используя ма-

лые предприятия. Вот как эти преступники окружают бизнес со всех сторон, и потребность в сильной ИТ-безопасности стала самой важной вещью для поддержания на рынке для бизнеса.

Как обеспечить безопасность

Поскольку кибербезопасность стала главной угрозой для бизнеса во всем мире, компании начали нанимать профессионалов, чтобы справиться с ней. Тем не менее, малые предприятия, которые все еще находятся на своем горящем уровне, не могут получить услуги профессионалов для защиты своего бизнеса от таких угроз.

Для владельцев малого бизнеса я перечисляю некоторые из экономически эффективных способов, с помощью которых они могут в некоторой степени защитить свою цифровую сеть.

– Обеспечьте безопасность информации вашего персонала, такой как пароли и имена пользователей.

– Организуйте надлежащий тренинг и расскажите своим сотрудникам о мерах предосторожности, которые они должны принимать при использовании устройств компании.

– Держите свои компьютеры в актуальном состоянии и всегда используйте платные антивирусные и шифровальные программы для максимальной безопасности.

– Если вы предоставляете мобильные устройства своим сотрудникам, то стандартизируйте их.

– Продолжайте обновлять безопасность на устройствах сотрудников.

– Меняйте пароли своих компьютеров и каждой учетной

записи, которую вы используете, каждые 60 дней и убедитесь, что измененный пароль сильнее предыдущих.

– Не позволяйте каждому иметь доступ к конфиденциальным документам компании. Разрешайте доступ только по необходимости.

– Если вы не можете нанять их на постоянной основе, по крайней мере, нанимайте специалистов по кибербезопасности на контрактной основе в течение 2—3 месяцев каждый год, чтобы они могли помочь вашей ИТ-безопасности.

Потребность в специалистах по кибербезопасности

Мы используем технологии каждый день практически для всего-от банковского дела до эксплуатации автомобилей, бытовой техники. Это стало очень важной тканью в нашей жизни. Однако большинство людей не понимают, что компьютеры, которые используются для выполнения большинства этих задач, очень небезопасны.

Киберпреступность уже не редкое явление. Эти так называемые кибер-вторжения становятся все более опасными и изощренными. Компании и люди становятся мишенью для конфиденциальных данных, таких как коммерческая тайна, финансовая и медицинская информация и т. Д. Существует необходимость в решении всепроникающей и постоянно развивающейся киберугрозы, которая привела к эволюции так называемых специалистов по кибербезопасности.

Согласно Gartner, *«Кибербезопасность охватывает широкий спектр практик, инструментов и концепций, тесно связанных с безопасностью информационных и операционных технологий. Кибербезопасность отличается тем, что включает наступательное использование информационных технологий для атаки противников.* Специалисты по кибербезопасности-это те, кто использует эти инструменты и концепции для предотвращения киберпреступности.

Резкое увеличение числа киберпреступлений в последние годы привело к экспоненциальному росту спроса на специалистов по кибербезопасности. ISACA, глобальная правозащитная группа по безопасности, прогнозирует, что к 2019 году в мире будет ощущаться нехватка 2 миллионов специалистов по кибербезопасности. Этой информации достаточно, чтобы привлечь внимание к этой области. Однако для того, чтобы войти и преуспеть в этой очень полезной, но требовательной отрасли, вы должны, по крайней мере, иметь следующий набор навыков:

– Хорошее понимание компьютера и сетей является обязательным

– Сосредоточьтесь на деталях

– Сильные аналитические навыки

– Непрерывное обучение

Кроме того, существует несколько сертификатов, которые позволяют вам продемонстрировать свои навыки и оставаться впереди. Некоторые из наиболее значимых из них следующие:

CISA (Certified Information Security Auditor): Это всемирно известный сертификационный курс, который позволяет получить знания, информацию и опыт для выявления критических проблем в различных видах информационных систем. Наличие этого сертификата подтверждает знания, которые вы приобрели для решения динамичных задач в области безопасности информационных систем (включая ки-

бербезопасность).

CISA проводится во всем мире и управляется ISACA, которая является некоммерческой организацией, специализирующейся исключительно на управлении ИТ. Учебная программа разделена на 5 основных областей/областей практики:

– Домен 1: Процесс аудита информационных систем

– Домен 2: Управление и управление ИТ

– Домен 3—Приобретение, разработка и внедрение информационных систем

– Домен 4—Операции, обслуживание и управление информационными системами

– Домен 5—Защита информационных активов

CISM (Certified Information Security Manager): Это также признанный сертификационный курс, который позволяет продемонстрировать свой опыт в управлении безопасностью информационных систем. Обладание этой сертификацией признает способность управлять, контролировать, оценивать и проектировать методы и системы информационной безопасности для предприятия.

CISM также проводится во всем мире и регулируется ISACA. Учебная программа разделена на 4 основные области/области практики:

– Домен 1—Управление информационной безопасностью

– Домен 2—Управление информационными рисками

– Домен 3—Разработка и управление программами ин-

формационной безопасности

– Домен 4—Управление инцидентами информационной безопасности

CISSP (Certified Information Systems Security Professional): Это независимая сертификация, проводимая и управляемая Международным консорциумом по сертификации безопасности информационных систем, более известным как (ISC) 2. Это высоко ценится из-за его уровня сложности (6 часов экзамена) и окупаемости инвестиций (занимает 4^{-e} место среди самых высокооплачиваемых сертификатов в разных отраслях). CISSP training предоставляет специалистам по информационной безопасности объективную меру компетентности и всемирно признанный стандарт достижений.

Учебный план CISSP делится на следующие области:

– Домен 1 – Безопасность и управление рисками

– Домен 2 – Безопасность активов

– Домен 3 – Инженерия безопасности

– Домен 4 – Коммуникационная и сетевая безопасность

– Домен 5 – Управление идентификацией и доступом

– Домен 6 – Оценка и тестирование безопасности

– Домен 7 – Операции безопасности

– Домен 8 – Разработка и безопасность программного обеспечения

Поскольку все вышеупомянутые курсы сложны и требуют значительной подготовки, на современном рынке существу-

ют веб-курсы и курсы под руководством инструкторов, которые помогут вам ускорить процесс и увеличить ваши шансы на успех.

Теперь, когда вы знаете, какие навыки необходимы для того, чтобы стать успешным специалистом по кибербезопасности, и как их получить, вам следует обратиться к крупным медицинским, финансовым, глобальным производственным организациям и консалтинговым фирмам, таким как Deloitte, PWC, EY, KPMG за карьерными возможностями.

Надеюсь, эта информация поможет вам начать работу!

4 столпа кибербезопасности для вашей организации

Крайне важно понять важные краеугольные камни кибербезопасности, чтобы ваша организация была наименее уязвима для растущих кибератак.

Информация и данные – это спасательный круг любого бизнеса сегодня. От деталей ваших сотрудников до ваших клиентов и продуктов, каждая бизнес-деталь находится в данных. Любая кража данных может не только оставить вас уязвимыми, но и может означать, что клиенты больше не доверяют своим данным, а вы выводите вас из бизнеса. Поэтому для предприятий крайне важно иметь проверки кибербезопасности и быть готовыми к любой такой попытке кражи данных. Хорошо разработанный план кибербезопасности должен основываться на следующих 4 основных столпах, обеспечивающих безопасность данных.

Столп I: политика и планирование

Без правильной политики трудно выделить правильный бюджет на кибербезопасность.

Первым столпом эффективной кибербезопасности является обеспечение наличия четкой политики кибербезопасности, детализирующей все аспекты. Политики и процедуры определяют, как эффективно применять различные технологические решения безопасности. С четко определенной политикой предприятия не будут рисковать низкими бюджетами на кибербезопасность или кибераналитику.

Идеальная политика безопасности должна иметь определенное правило соотношения риска и затрат, которое может быть применено к другим политикам и процедурам внутри предприятия. Политика не должна определять технологию, которая будет использоваться, поскольку технологии постоянно меняются и совершенствуются со временем. Некоторые предприятия даже приняли несколько политик безопасности, по одной для каждого сегмента или подразделения в соответствии с факторами риска предприятия и его домена.

Столп II: использование технологий и бдительная внутренняя безопасность

Технологические эксперты должны вступить в игру, чтобы выбрать правильный набор инструментов для защиты организации от любого кибер-нарушения.

После того, как организация разработала политику безопасности, следующий шаг включает в себя поиск подходящей технологии для ее потребностей в области безопасности. Оценка технологий может потребовать участия **экспертов по кибербезопасности и кибераналитике** в поиске наилучших доступных инструментов. Решение об использовании адекватных инструментов, таких как процессы идентификации пользователей, системы, оборудование, контроль доступа, шифрование данных, брандмауэры, программы защиты от вирусов и т. Д., подпадает под сферу применения технологий.

Основанные на технологиях инструменты кибербезопасности являются про активными, поскольку они постоянно отслеживают любые изменения в нормальной функциональности процессов. С другой стороны, они могут быть доступны хакерам. Всего лишь одного небольшого входа в системы безопасности или небольшого нарушения может быть доста-

точно, чтобы вызвать отключение таких инструментов безопасности. Технологические инструменты требуют постоянного мониторинга и бдительной внутренней команды экспертов по безопасности для обеспечения всесторонней защиты данных.

Столп III: образование и осведомленность сотрудников

Хорошо информированные сотрудники могут помочь организациям использовать весь потенциал политик и технологий безопасности.

Предприятие может иметь правильную политику безопасности и использовать правильные технологии, но, если человеческий ресурс не знает и не мотивирован, все это может сойти на нет. Поэтому еще одним важным столпом безопасности является обучение и распространение осведомленности о кибербезопасности и кибераналитике.

Обучение сотрудников распознаванию «плохого», предлагая обмен информацией в режиме реального времени, может иметь большое значение для предотвращения рисков. Мошеннические электронные письма, фишинг и открытие нежелательных вложений электронной почты по-прежнему являются основными причинами, позволяющими хакерам войти или получить доступ. Благодаря повышению осведомленности сотрудников такое поведение можно контролировать, что приводит к улучшению аналитики безопасности.

Недавно печально известная крипто-вредоносная программа или вымогатель «Wannacry» является типичным примером нарушения данных, которое имело свои корни в открытии вредоносных вложений электронной почты.

Здесь потребность в специалистах по кибербезопасности возрастает для защиты данных от хакеров, информируя сотрудников и обучая их аспектам кибербезопасности, предприятие может существенно минимизировать свои риски безопасности.

Столп IV: резервное копирование и аварийное восстановление

Как ни странно, это наиболее актуально в сегодняшнее время растущих кибератак.

В качестве последней линии защиты от любой атаки данных ваше предприятие должно иметь хорошее решение для обеспечения непрерывности бизнеса и аварийного восстановления. Следует поощрять наличие копий данных, хранящихся в нескольких местах, которые находятся вне сайта и резервируются ежечасно каждый день.

Убедитесь, что ваш поставщик решений для восстановления данных и развития бизнеса предлагает адекватную и регулярную проверку резервного копирования на возможность восстановления данных. Стимулируйте наихудший сценарий, отключая сервер и ища резервную копию данных, чтобы убедиться, что вы всегда готовы к любой возможности нарушения данных. Стимуляция также может гарантировать отсутствие паники, и каждый сотрудник знает свою роль во время любой кибератаки, чтобы обеспечить минимальное время простоя и повлиять на важные данные и услуги.

Вывод: Кибербезопасность сегодня является неотъемлемой частью любой корпоративной функциональности. Независимо от того, насколько велико или мало, каждое предприятие уязвимо. Следуя четырем столпам безопасности,

организация может сохранить свою структуру безопасности на месте, чтобы свести к минимуму такие угрозы.

Топ-10 навыков, чтобы стать этичным хакером

С переходом отраслей на облачные платформы для работы и хранения критической информации кибербезопасность становится растущей проблемой всех отраслей. Недавнее нарушение данных в Adobe Systems привело к потере личных данных почти на 3 миллиона своих клиентов. В качестве превентивной меры ведущие ИТ-компании, такие как IBM, инвестируют кроры в защиту своей информации. Вот где этический взлом входит в картину. Процесс поиска слабых мест и уязвимостей существующих информационных систем или компьютеров и тем самым помочь компаниям улучшить свои системы безопасности известен как этический взлом. Часто этический взлом идет по тому же пути, что и хакеры/злоумышленники, копируя их методологии и инструменты. Он также известен как тестирование на проникновение, тестирование на вторжение или red teaming.

Кто такой этический хакер?

Этический хакер или хакер – whitehat-это профессионал в области безопасности, использующий навыки взлома в оборонительных целях для проверки состояния безопасности информационных систем организаций. Этический хакер в первую очередь ищет следующую информацию:

– Каковы лазейки, такие как информация, местоположения или системы, к которым злоумышленник может получить доступ?

– Что может увидеть злоумышленник с этой информацией?

– Что может сделать злоумышленник с имеющейся информацией?

– Кто-нибудь уже замечает или реагирует на такие попытки в информационных системах?

Цифровая трансформация и новые технологии, такие как блокчейн, Интернет вещей (IoT), увеличили спрос на этических хакеров. Payscale сообщает, что средняя зарплата сертифицированного этического хакера составляет $92000 в США и 483 875 Рупий в Индии.

Итак, что нужно, чтобы стать этическим хакером?

Топ-10 навыков, чтобы стать этичным хакером

1. Отличные навыки работы с компьютером

Это может показаться базовым навыком, но очень важно стать этичным хакером. Нужно быть очень быстрым в обращении с базовыми навыками, связанными с управлением системой, и твердо держаться за командную строку в Windows/операционном обеспечении, редактировать реестр и устанавливать свои сетевые параметры.

2. Навыки программирования

Чтобы получить доступ к основам программного обеспечения, необходимо иметь правильное понимание различных языков программирования, используемых для его разработки. Наиболее распространенными языками являются Python, SQL, C, C++ и Perl.

3. Системы управления базами данных (СУБД)

СУБД-это суть создания и управления всеми базами данных. Доступ к базе данных, где хранится вся информация, может поставить компанию под огромную угрозу, поэтому важно обеспечить защиту этого программного обеспечения от взлома. Этический хакер должен хорошо понимать это, а также различные механизмы баз данных и схемы данных, чтобы помочь организации создать сильную СУБД.

4. Linux

Поскольку большинство веб-серверов работают на операционной системе Linux, получение доступа к этому серверу для проверки лазеек является еще одним обязательным навыком для этических хакеров. Понимание операционных систем, таких как Redhat, Ubuntu, Fedora, их команд и GUI (графический интерфейс пользователя), даст вам большие рычаги воздействия.

Конец ознакомительного фрагмента.