Trustworthy Computing (TwC)

Кузьмин Егор Витальевич, студент группы НКАбд-03-23

Содержание

Список иллюстраций

Список таблиц

1 Предпосылки создания

Предпосылки создания системы Trustworthy Computing (TwC) в Microsoft глубоко укоренены в истории развития интернета и цифровых технологий, особенно в контексте безопасности эксплуатации программного обеспечения. До середины 1990-х годов интернет воспринимался в основном как академический и исследовательский ресурс, но к концу десятилетия он стал чрезмерно массовым явлением, что привело к резкому увеличению в нем количества пользователей и коммерческой деятельности соответственно. Одним из главных моментов для корпорации стал выпуск Windows 95, который изначально не включал веб-браузер из-за недопонимания относительно быстрого роста популярности интернета. Однако вскоре после этого Microsoft активизировала свои усилия в интернет-пространстве, запустив свой веб-сервер и онлайн-сервис MSN. В конце 1990-х и начале 2000-х годов компания столкнулась с серьезными проблемами безопасности, связанными с распространением вредоносных программ, включая вирусы и черви, такие как Code Red, Nimda, Klez и Slammer, которые активно появлялись в то время. Эти атаки не только причинили значительный ущерб пользователям, но и подорвали доверие к продуктам Microsoft, особенно среди крупных корпоративных клиентов, таких как правительственные агентства и финансовые учреждения. В частности, вирус Code Red, названный мною ранее, появившийся в 2001 году, использовал уязвимости в серверах Microsoft IIS для своего распространения, что привело к значительным финансовым потерям компании и нарушению работы многих систем. Следом за ним, червь Nimda использовал уже несколько методов для своего распространения, в том числе за-

ражение через электронную почту и просмотр веб-страниц, что дополнительно усугубило ситуацию с безопасностью в сети.

2 Решение проблем

Вышеописанные события подчеркнули необходимость в более строгом подходе к безопасности и надежности программного обеспечения. В ответ на эти вызовы и в целях восстановления доверия клиентов, в январе 2002 года Билл Гейтс направил всем сотрудникам Microsoft памятку, в которой объявил о запуске инициативы Trustworthy Computing. Эта инициатива призвана была радикально изменить подход компании к разработке программного обеспечения, сделав безопасность, приватность и надежность, а также этику ведения бизнеса центральными аспектами всех продуктов и услуг Microsoft, некими столпами. Одним из ключевых аспектов данной программы стало введение процесса Patch Tuesday, который начал действовать с 2003 года и предполагал регулярное ежемесячное выпускание обновлений безопасности для всех продуктов компании, что позволило пользователям более предсказуемо управлять обновлениями и повысить общий уровень уверенности в системах. Кроме того, была разработана и внедрена методология Security Development Lifecycle (SDL), что расшифровывается как жизненный цикл разработки безопасного программного обеспечения, являющаяся ключевым элементом инициативы Trustworthy Computing. [1]

3 SDL

SDL представляет собой комплексную методологию, включающую в себя ряд процессов и практик, направленных на обеспечение безопасности и надежности программного продукта на всех этапах его жизненного цикла, начиная от концепции и заканчивая развертыванием и поддержкой. Основной целью является снижение количества и серьезности уязвимостей в программном обеспечении путем интеграции мероприятий по обеспечению безопасности на ранних стадиях разработки. Это позволяет предотвращать потенциальные угрозы безопасности до того, как программное обеспечение будет выпущено, тем самым снижая риски для конечных пользователей и уменьшая затраты на исправление ошибок после выпуска продукта. SDL включает в себя следующие ключевые аспекты: => На начальном этапе разработки проекта формулируются требования к безопасности, основанные на анализе потенциальных угроз и рисков для конкретного продукта. => На этапе проектирования акцент делается на создании архитектуры, устойчивой к угрозам, путем применения принципов минимализации привилегий, разделения обязанностей и других практик. => Используются специализированные инструменты для автоматизированного поиска потенциальных уязвимостей в исходном коде на ранних этапах разработки. => Проведение пенетрационного тестирования, динамического анализа и других видов проверок безопасности для выявления уязвимостей, которые не могут быть обнаружены статическими методами. => Разработка процедур и инструментов для обеспечения безопасности продукта в процессе его развертывания и последующей эксплуатации пользователем. => Создание четких процедур реагирова-

ния на инциденты безопасности, включая обновление программного обеспечения и информирование пользователей о способах защиты от угроз. Применение SDL позволило Microsoft значительно повысить уровень безопасности своих продуктов и стало примером для всей индустрии. Многие компании оценили успех, (например Addobe и Cisco) и адаптировали аналогичные принципы уже для своих собственных процессов разработки программного обеспечения, что подтверждает важность и эффективность подхода, ориентированного на безопасность на всех этапах жизненного цикла разработки. [2]

4 Blue Hat

TwC также подчеркнула значение сотрудничества как внутри компании, так и с внешними экспертами и исследователями в области кибербезопасности, что является немаловажным для более эффективного выявления и устранения угроз. Проведение конференций “Blue Hat”, на которых специалисты данной области могли напрямую взаимодействовать с разработчиками Microsoft, а также создание программы вознаграждения за обнаружение уязвимостей стали важными шагами на пути к повышению безопасности продуктов компании. Эти мероприятия были названы в честь “синих шапочек” (отсылка к термину “blue team”, используемому в профессиональной среде для обозначения группы, защищающей систему), а также “черных шапочек” (отсылка к “black hat”, термину для обозначения хакеров, занимающихся поиском уязвимостей для вредоносных целей), что символизирует смешение этих двух сторон для совместной работы. Основная цель конференций Blue Hat - способствовать открытому диалогу и обмену знаниями между Microsoft и внешним сообществом специалистов по безопасности соответсвенно, что предоставляет внешним экспертам возможность прямо донести до разработчиков Microsoft информацию о последних методах и техниках атак, а также об уязвимостях, которые они обнаружили. С другой стороны, инженеры и разработчики Microsoft могут поделиться своим опытом создания защищенных продуктов и практиками, которые они используют для обеспечения защиты своих систем. Мероприятия Blue Hat также служат в качестве инструмента для повышения осведомленности внутри компании о важности и сложности вопросов кибербезопасности. С мо-

мента своего создания конференции Blue Hat сыграли важную роль в процессе улучшения практик безопасности в Microsoft, а также способствовали созданию более тесных связей между корпорацией и широким сообществом специалистов данной сферы. Они стали частью широкой инициативы по вовлечению внешних исследователей в процесс улучшения безопасности, что включает в себя такие программы, как Bug Bounty, и практику координированного раскрытия уязвимостей. [3]

5 Выводы

В заключение, инициатива Trustworthy Computing - это не просто набор политик или практик, а смена парадигмы к приоритизации безопасности, приватности и надежности.

Взгляд в будущее показывает, что принципы Trustworthy Computing остаются актуальными как никогда. Распространение облачных вычислений и увеличение интеграции информационных технологий в каждый аспект повседневной жизни подчеркивают необходимость создания соответствующих продуктов. Концепция Microsoft заложила прочную основу, но путь продолжается, поскольку возникают новые вызовы и возможности, технологический ландшафт непрерывно развивается.

Список литературы

[1][“Trustworthy-computing-initiative”](https://mcpmag.com/articles/2004/02/09/will-trustworthy-computing-last.aspx) [2][“Microsoft-Trustworthy-computing-initiative: anniversary of 10 years”](https://news.microsoft.com/2012/01/12/at-10-year-milestone-microsofts-trustworthy-computing-initiative-more-important-than-ever/) [3][“Celebrating 20 years of trustworthy-computing-initiative”](https://www.microsoft.com/en-us/security/blog/2022/01/21/celebrating-20-years-of-trustworthy-computing/)