

Доклад на тему «Trustworthy Computing Initiative»

Дисциплина: Операционные системы

Бражко Александра Александровна

Содержание

1 Введение	5
2 Основная часть	6
2.1 Основные принципы TWC	6
2.2 Реализованные стратегии	7
2.3 Достигнутые результаты	9
2.4 Влияние на индустрию информационных технологий	10
3 Заключение	12
Список литературы	13

Список иллюстраций

2.1	Ключевые столпы TWC	7
2.2	Реализованные цели TWC	9
2.3	Достигнутые результаты	10
2.4	TWC	11

Список таблиц

1 Введение

В начале 2000-х годов компания Microsoft столкнулась с серьезными вызовами в области безопасности, приватности и надежности своих продуктов. Широкое распространение вредоносного ПО, уязвимости в операционных системах и растущая критика со стороны пользователей и экспертов побудили компанию к принятию кардинальных мер.

В 2002 году Билл Гейтс объявил о запуске Trustworthy Computing Initiative (TWC), ставшей одним из наиболее значимых шагов в истории Microsoft. Значение и влияние TWC охватывают не только Microsoft, но и юридические и экономические аспекты, а также “человеческий фактор”. [1]

Целью данного доклада является анализ инициативы Trustworthy Computing, ее основных принципов, реализованных стратегий, достигнутых результатов и ее влияния на индустрию информационных технологий.

2 Основная часть

2.1 Основные принципы TWC

Билл Гейтс обозначил четыре ключевых столпа инициативы TWC (рис. 2.1).

Надежность (Reliability): Обеспечение стабильности, предсказуемости и доступности программного обеспечения. Это включает в себя улучшение качества кода, повышение устойчивости к ошибкам и предоставление средств для восстановления после сбоев.

Безопасность (Security): Защита систем и данных от несанкционированного доступа, использования, раскрытия, нарушения, изменения или уничтожения. Это включает в себя как защиту от внешних угроз (хакеры, вирусы), так и защиту от внутренних ошибок в программном коде.

Конфиденциальность (Privacy): Предоставление пользователям контроля над их личными данными и прозрачность в отношении того, как эти данные собираются, используются и передаются. Microsoft обязуется соблюдать правила конфиденциальности и предоставлять пользователям инструменты для управления их данными.

Деловая этика (Business Integrity): Следование этическим принципам и бизнес-практикам при разработке, продаже и поддержке программного обеспечения. Это включает в себя честность, прозрачность и ответственность перед пользователями. [2]

TRUSTWORTHY COMPUTING

Four Pillars of Trustworthy Computing



Рис. 2.1: Ключевые столпы TWC

2.2 Реализованные стратегии

Для реализации принципов TWC, Microsoft предприняла ряд стратегических шагов (рис. 2.2):

Переобучение разработчиков. Был организован масштабный процесс обучения и переквалификации разработчиков, чтобы они уделяли больше внимания безопасности и качеству кода. Внедрены практики безопасной разработки (Secure Development Lifecycle - SDL).

Аудит кода и обнаружение уязвимостей. Существенно увеличены инвестиции в инструменты и методы для автоматического и ручного аудита кода с целью обнаружения уязвимостей на ранних стадиях разработки. Использовались методы статического и динамического анализа кода.

Сотрудничество с сообществом. Компания Microsoft начала более активно сотрудничать с экспертами по безопасности, исследовательскими организациями и хакерами-этиками (white hat hackers) для выявления и устранения уязвимостей.

Были организованы программы Bug Bounty для стимулирования обнаружения уязвимостей.

Интеграция безопасности в продукты. Безопасность стала рассматриваться как неотъемлемая часть продукта, а не как дополнение. В Windows были внедрены новые функции безопасности, такие как Firewall, User Account Control (UAC) и Data Execution Prevention (DEP).

Улучшение процесса выпуска обновлений. Разработана более эффективная система распространения патчей и обновлений безопасности (Windows Update), чтобы оперативно устранять обнаруженные уязвимости.

Создание специализированных команд. Созданы специальные команды, ответственные за безопасность и конфиденциальность на всех этапах разработки.

[3]

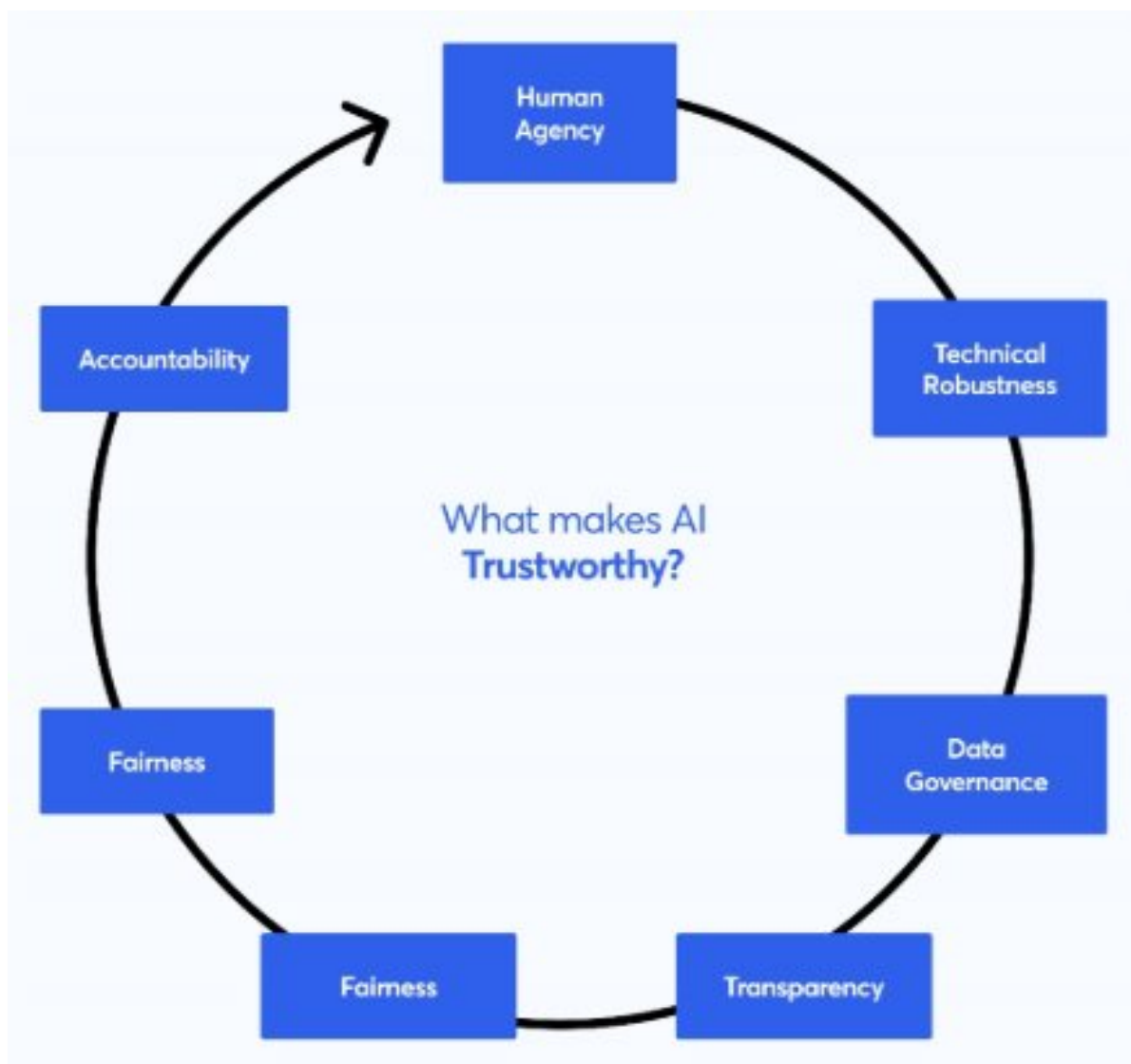


Рис. 2.2: Реализованные цели TWC

2.3 Достигнутые результаты

Благодаря TWC продукты компании Microsoft значительно улучшились в сферах безопасности, надежности и конфиденциальности (рис. 2.3).

Заметно снизилось количество и серьезность обнаруженных уязвимостей в программном обеспечении Microsoft. Внедрение практик SDL привело к улучшению качества кода и снижению количества ошибок. Windows стала гораздо

более безопасной операционной системой, чем это было до TWC. Инициатива помогла восстановить и укрепить доверие пользователей к продуктам Microsoft. Активное сотрудничество с сообществом и разработка инструментов для анализа безопасности способствовали созданию более безопасной экосистемы для всех пользователей Windows.

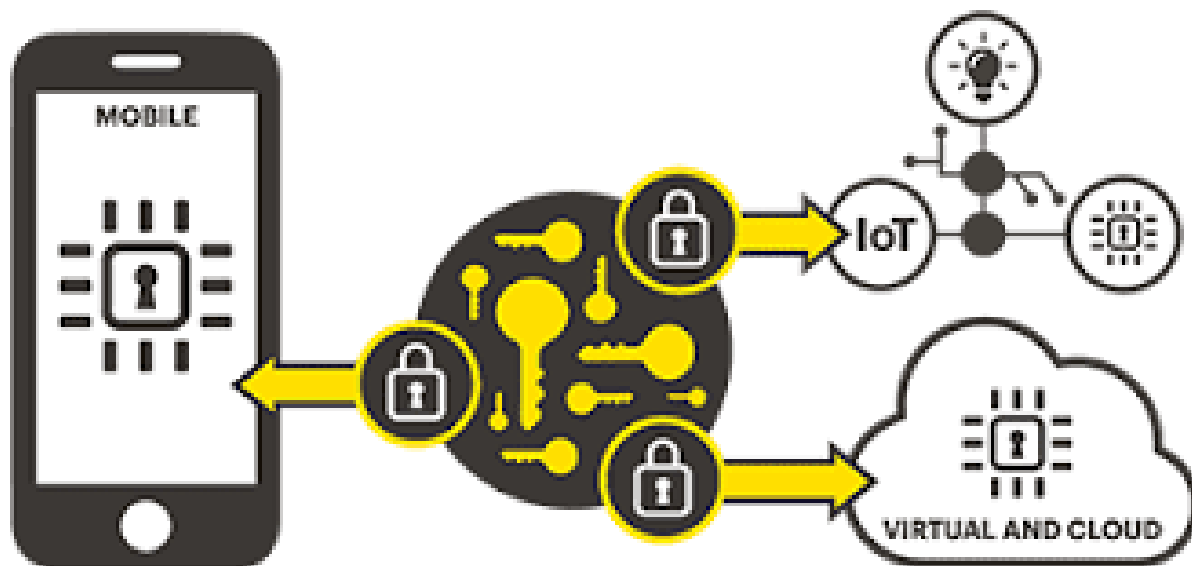


Рис. 2.3: Достигнутые результаты

2.4 Влияние на индустрию информационных технологий

TWC оказала большое влияние на всю индустрию информационных технологий (рис. 2.4).

Инициатива привлекла внимание к важности безопасности и конфиденциальности в разработке программного обеспечения, что побудило другие компании инвестировать в эти области. Многие компании начали внедрять практики безопасной разработки, аналогичные SDL, чтобы повысить безопасность своего программного обеспечения. TWC стимулировала развитие индустрии безопасности, включая разработку новых инструментов и методов для анализа и защиты

программного обеспечения. Более того распространилось влияние на область конфиденциальности, заставив компании более внимательно относиться к защите личных данных пользователей. Многие практики, разработанные в рамках TWC, стали де-факто стандартами в индустрии.



Рис. 2.4: TWC

3 Заключение

Trustworthy Computing Initiative была важным шагом в развитии индустрии информационных технологий. Она заставила Microsoft пересмотреть свои подходы к разработке программного обеспечения и уделять больше внимания безопасности, конфиденциальности и надежности. Хотя TWC не была безупречной, она оказала значительное положительное влияние на безопасность и качество программного обеспечения Microsoft и способствовала повышению осведомленности о безопасности во всей индустрии. Она стала важным прецедентом и оказала влияние на развитие практик безопасной разработки по всему миру.

Список литературы

1. Взгляд Microsoft на построение защищённых систем [Электронный ресурс]. 2005. URL: https://fcenter.ru/online/hardarticles/os/12461-Vzglyad_Microsoft_na_postroenie_z
2. 10 years of Microsoft's Trustworthy Computing Initiative [Электронный ресурс]. 2012. URL: <https://www.helpnetsecurity.com/2012/01/13/10-years-of-microsofts-trustworthy-computing-initiative/>
3. Celebrating 20 Years of Trustworthy Computing [Электронный ресурс]. 2022. URL: <https://www.microsoft.com/en-us/security/blog/2022/01/21/celebrating-20-years-of-trustworthy-computing/>.