Аладдин РД

Средство доверенной загрузки TSM

Современные угрозы и средства защиты уровня базовой системы ввода-вывода

01.12.2013

Доверенная вычислительная среда

- Доверенная среда - область существования и функционирования доверенных компонентов, в пределах которой обеспечиваются необходимые условия непрерывности их жизнедеятельности и поддержания требуемого уровня доверия на всем протяжении жизненного цикла (Всероссийская конференция «Инфокоммуникационные технологии в научных исследованиях» г. Таруса, 14-16 ноября 2012 года).

Вредоносное ПО уровня BIOS, UEFI и т.д.

- Появляется новое вредоносное ПО, способное заражать BIOS, CMOS работать ниже уровня операционной системы и компрометировать систему на уровне «железа».
- Загрузка (обновление) вредоносного буткит-кода может осуществляться с удаленного сервера каждый раз при старте компьютера.
- Невозможно определить стандартными средствами, не остается каких-либо следов на жестком диске.
- Компьютерная система остается скомпрометированной даже после полной переустановки ОС и смены жёсткого диска.

Пример:

- В августе 2012 г. на конференции Black Hat французским исследователем компании eScan было представленно новое вредоносного ПО способное подменять собой BIOS - **буткит Rakshasa.**
- Rakshasa работает на 230 моделях материнских плат и успешно избежал обнаружения при проверки 43-мя антивирусами.
- Rakshasa способен заражать не только BIOS но и прошивки других периферийных устройств.

Закладки уровня BIOS, UEFI и т.д.

- Недокументированные функции (“Закладки”) установленные производителями оборудования.

Пример:

- В марте 2013 г. американский оператор сотовой связи Sprint Nextel и ее японский партнер Softbank отказались от закупок продукции китайской компании Huawei.
- Комитет по разведке палаты представителей США выпустил доклад, в котором назвал телекоммуникационное оборудование, выпускаемое китайскими компаниями, угрозой для безопасности страны в связи с тем, что оно может скрывать в себе недокументированные функции для перехвата и анализа сетевого трафика.

Последствия реализации угроз

- Нарушение конфиденциальности, целостности и доступности информации (в том числе ограниченного доступа) в обход стандартных средств обеспечения безопасности.
- Кража логинов, паролей от учётных записей информационных систем, похищение данных кредитных карт.
- Предоставление злоумышленнику удаленного доступа к носителям информации и ресурсам компьютера.
- Блокирование компьютера пользователя (или шифрование его файлов) с целью получения выкупа.
- Запуск скрытых виртуальных машин, перехват, анализ и фильтрация сетевого трафика.
- Включение компьютера в ботнет.
- Дистанционный вывод оборудования из строя по удаленной команде.

Моделирование угроз на объекте

- Загрузка нештатной операционной системы для обхода правил разграничения доступа штатной операционной системы и (или) других средств защиты информации, работающих в среде штатной операционной системы.
- Несанкционированная загрузка штатной операционной системы и получение несанкционированного доступа к информационным ресурсам.
- Нарушение целостности программной среды средств вычислительной техники и (или) состава компонентов аппаратного обеспечения СВТ.

Предположения о нарушителе

- Администратор безопасности не является нарушителем.
- Нарушитель имеет доступ к средствам вычислительной техники информационной системы.
- Нарушитель обладает техническими знаниями относительно реализованных функциональных возможностей средств доверенной загрузки, применяемых в информационной системе.
- Нарушитель не осуществляет действий, направленных на нарушение физической целостности средств вычислительной техники, доступ к которым контролируется с применением средств доверенной загрузки.

Существующие средства защиты

- Аппаратные средства доверенной загрузки.
- Средства доверенной загрузки уровня базовой системы ввода-вывода.
- Средства доверенной загрузки уровня загрузочной записи.

Функции безопасности (ФБ) СДЗ

- Разграничение доступа к управлению средством доверенной загрузки.
- Управление работой средства доверенной загрузки.
- Управление параметрами средства доверенной загрузки.
- Аудит безопасности средства доверенной загрузки.
- Идентификация и аутентификация.
- Тестирование средства доверенной загрузки, контроль целостности программного обеспечения и параметров средства доверенной загрузки.
- Контроль компонентов средства вычислительной техники.
- Блокирование загрузки средством доверенной загрузки.
- Управление доступом к ресурсам средства вычислительной техники.
- Сигнализация средства доверенной загрузки.
- Обеспечение безопасности средства доверенной загрузки при возникновении сбоев и ошибок в процессе работы.
- Обеспечение безопасности после завершения работы средства доверенной загрузки.

Требования регуляторов к ИС по СДЗ

- Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (Приказ ФСТЭК № 17 от 11.02.2013г.).
- Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (Приказ ФСТЭК №21 от 18.02.2013г.).

Обозначение и номер требуемых мер:

- УПД.17 «Обеспечение доверенной загрузки СВТ»;
- ЗСВ.5 «Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией».

Мы всегда поможем

Адрес:129226, Москва, ул. Докукина, д. 16, корп. 1

Телефоны:

+7 (495) 223-0001 (многоканальный)

+7 (495) 988-4640

Факс:+7 (495) 646-0882

E-mail:aladdin@aladdin-rd.ru

http://www.aladdin-rd.ru