ТЕХНИЧЕСКИ УНИВЕРСИТЕТ - СОФИЯ
СТОПАНСКИ ФАКУЛТЕТ
КАТЕДРА „ИКОНОМИКА, ИНДУСТРИАЛЕН ИНЖЕНЕРИНГ И МЕНИДЖМЪНТ“

З А Д А Н И Е

По

НСЕККС

Тема: Организиране сигурността на софтуера

на студента:	Николай Георгиев Синоров	**група:**	***55***	**Ф№**	161219049

СОФИЯ
2023 г.

Софтуерната сигурност софтуерът за сигурност е всеки тип софтуер, който защитава компютър, мрежа или всяко компютърно устройство. Той управлява контрола на достъпа, осигурява защита на данните, защитава системата от вируси и проникванията, базирани на мрежа / Интернет, и защитава от други рискове за сигурност на ниво система.

Софтуерът за сигурност може да защити компютъра от вируси, злонамерен софтуер, неоторизирани потребители и други експлоатационни мерки за сигурност, произхождащи от Интернет.

Видовете софтуер за сигурност включват антивирусен софтуер, защитна стена, софтуер за мрежова защита, софтуер за интернет защита, софтуер за премахване и защита от злонамерен / спам софтуер, криптографски софтуер и др.

В компютърните среди на крайните потребители антивирусният и анти-спам софтуерът е най-разпространеният тип използван софтуер, докато корпоративните потребители добавят защитна стена и система за откриване на проникване отгоре.

Причините, водещи до функционално неподходящ резултат, могат да бъдат различни:

- неизправности в компютърните системи
- грешки на програмисти и оператори
- дефекти в софтуера

Дефектите се считат за два вида:

- умишлени - резултат от злонамерени действия
- непреднамерени - погрешни човешки действия

Компютърна сигурност е клон на информационната сигурност с приложение в компютрите и компютърните мрежи. Основна цел на компютърната сигурност е защита на информацията и хардуера от кражба и повреждане.

Термини за сигурност на софтуера

- Неволен дефект - обективно и (или) субективно образуван дефект, водещ до получаване на неверни решения (резултати) или нарушаване на функционалността на КС.
- Разрушаващ софтуер – съвкупност от програмни и/или технически средства, предназначен за нарушаване (изменение) на зададената технология за обработка на информация и/или целенасочено разрушаване извън вътрешното състояние на информационно-изчислителния процес в КС.
- Умишлен дефект – криминален дефект, внесен от субекта за целенасочено нарушение и (или) разрушаване на информационния ресурс.
- Средства на активно противодействие - средства за защита на информационния ресурс на КС, позволяващи блокиране на канала на изтичане на информация, разрушаване на действията на противника, минимизиране на нанесената щета и предотвратяване на последващо деструктивно действие на противника, посредством ответно въздействие на информационния ресурс.
- Несанкциониран достъп – действия, водещи до нарушаване на безопасността на информационния ресурс и получаване на секретни сведения.
- Нарушител (нарушители) - субект (субекти), извършващи неоторизиран достъп до информационния ресурс.
- Оценка на сигурността на софтуера – процес на получаване на количествени или качествени показатели на информационна сигурност при отчитане на преднамерени и непреднамерени дефекти в системата.

Технически и организационни средства за защита сигурността на софтуера

Безопасност (сигурност) на софтуера в широк смисъл е свойството му да функционира без проявления на различни негативни последствия за конкретната компютърна система или оборудване.

При изследване на проблемите за защита на софтуера от преднамерени дефекти е неизбежна постановката на следните въпроси:

- Кой потенциално може да осъществи практическо внедряване на програмни дефекти с разрушителното въздействие в изпълнимия програмен код?
- Какви са възможните мотиви за действието на субекта, осъществяващо разработката на такива дефекти?

- Как може да се идентифицира наличието на програмен дефект?
- Как може да се различи преднамерения програмен дефект от програмната грешка?
- Какви са най-вероятните последствия от активирането на деструктивните програмни средства при експлоатация на компютърните системи и техническите системи?

Въздействия от промяна на функционирането на компютърна система (мрежа):

- намаляване на скоростта на изчислителната система (мрежа);
- частично или пълно блокиране на системата (мрежата);
- имитация на физически (хардуерни) неизправности на изчислителните съоръжения и периферни устройства;
- препращане на съобщения;
- заобикаляне на софтуер и хардуер за преобразуване на криптографска информация;
- осигуряване на достъп до системата от непредвидени периферни устройства.

Въздействия от неразрешено четене на информация:

- четене на пароли и идентифицирането им с конкретни потребители;
- получаване на класифицирана информация;

- идентификация на исканата от потребителите информация;
- подмяна на пароли с цел достъп до информация;
- мониторинг на активността на абонатите на мрежата за получаване на косвена информация за взаимодействията на потребителите и естеството на информацията, обменяна от мрежови абонати.

Неправомерното модифициране на информация е най-опасната форма на програмни отметки, тъй като води до найопасните последици:

- унищожаване на данни и кодове на изпълними програми;
- правене на фини, трудни за откриване промени в информационните масиви;
- внедряване на програмни маркери в други програми и подпрограми (вирусен механизъм на действие);
- изкривяване или унищожаване на собствената информация на сървъра и по този начин прекъсване на мрежата;
- модификация на пакетите за съобщения.

Принципи за осигуряване на защитен софтуер:

- Тестване на софтуер, основаващо се на разработването на тестови комплекси, които могат да бъдат параметризирани на конкретни класове програми с възможност за функционален и статистически контрол в широк диапазон на изменение на входни и изходни данни.
- Провеждане на натурни изпитвания на програми при екстремални натоварвания със симулирано въздействие на активни дефекти.
- Профилактично извадково изпитване и пълно сканиране на софтуера за наличие на преднамерени дефекти.
- Разработка и експериментално тестване на средствата за верификация на програмни изделия.

Уязвимост на съвременните методи за защита и използване на автоматични средства за защита“

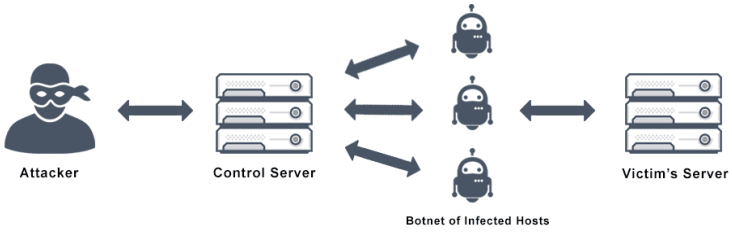
Уязвимостта е податливост или недостатък на системата. Уязвимост съществува, когато съществува най-малко едно работещо нападение или експлойт.

За да се подсигури една компютърна система, е важно да се разберат атаките, които могат да се направят срещу нея.

Тези заплахи могат да се класифицират в една от следните основни категории:

- „Задни врати“ - „Задна врата“ в компютърните системи, е всяка криптосистема или алгоритъм, които тайно заобикалят нормалните контроли за проверка на автентичността или сигурността. Те могат да съществуват поради различни причини. Те могат да бъдат добавени от оторизираната страна, с цел да позволи законен достъп или от нападател за злонамерени причини, но независимо от мотивите за тяхното съществуване, те са предпоставка за уязвимост.

- „Denial-of-service“ атаки - DoS атаките са проектирани да направят една машина или мрежов ресурс недостъпни за потребителите. Нападателите могат да спрат обслужването на отделни жертви, като например чрез умишлено въвеждане на грешна парола достатъчно последователни пъти предизвикващо блокиране на жертвата, или те могат да пренатоварят една машина или мрежа и да блокират всички потребители едновременно. Докато мрежовата атака от един IP адрес може да бъде блокирана чрез добавяне на ново правило в защитната стена, много форми на „Distributed denial of service“(DDoS) атаки са възможни, когато атаката идва от голям брой точки.



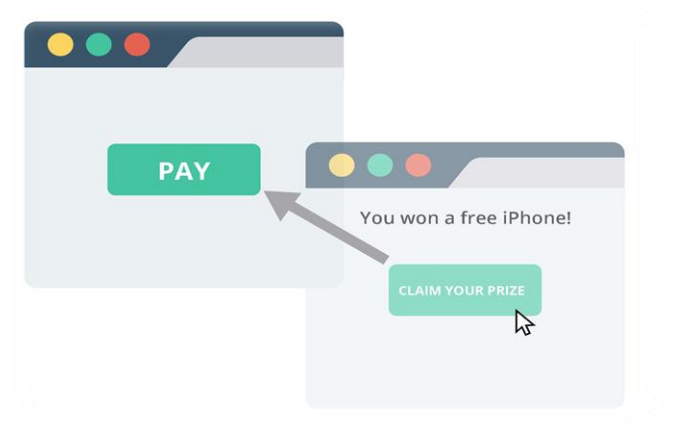
- Атаки с директен достъп - Неоторизиран потребител, който получава физически достъп до компютър, често е в състояние да изтегли директно данни от него. Той може да компрометира сигурността, като направи оперативни промени в системата, инсталира софтуерни червеи, кийлогъри, или устройства за прикрито слушане.
-

Други:

1. „Spoofing“ - е техника, при която един човек или програма успешно се представя за друг чрез фалшифициране на данни.

2. Фишинг - Фишинг е опитът да се придобие чувствителна информация като потребителски имена, пароли и информация за кредитни карти директно от потребителите. Фишингът обикновено се осъществява чрез имейл фишинг или мигновени съобщения, и то често насочва потребителите към въвеждане на данните в един фалшив уебсайт.

3. „Clickjacking“ - Clickjacking е злонамерена техника, при която един нападател лъже-потребителя прихваща натискане на бутон или връзка към друга уеб страница и го пренасочва. Това се прави с помощта на множество прозрачни или непрозрачни слоеве. Нападателят основно „отвлича“ кликванията, предназначени за страницата на най-високо ниво и маршрута им към някоя друга страница, най-вероятно притежавана от някой друг. Внимателното изготвяне е комбинация от стилове, вградени рамки, бутони и текстови полета, потребителят може да бъде накаран да вярва, че въвежда парола или друга информация в някоя автентични уеб страница, докато тя се насочва към една невидима рамка контролирана от нападателя.



Системи, които са обект на хакерски атаки:

1. Финансови системи - Уеб сайтове, които приемат номера на кредитни карти и банкови сметки са видни цели за хакерските атаки, поради възможността за незабавна финансова печалба от прехвърляне на пари, извършване на покупки, или продажба на информацията на черния пазар.

2. Потребителски устройства - Компютри контролират функциите на много помощни програми, включително координация на телекомуникациите, електрическата мрежа, атомните електроцентрали, както и отваряне на вентила и затваряне на водни и газови мрежи.

3. Големи корпорации – Големите корпорации са честа цел. В много случаи това е насочено към финансова изгода чрез кражба на самоличност и включва нарушения с данни, като например загубата на милиони данни за кредитни карти на клиенти

4. Правителство - Правителството и военните компютърни системи са често атакувани от активисти, както и чужди сили. Местните и регионални власти трафик контрола, полиция, разузнавателни, записи на персонала и финансови системи също са потенциални цели, тъй като те са вече до голяма степен компютризирани.

Средства за защита:

В компютърната сигурност контрамярката е действие, устройство, процедура, или техника, която намалява заплахата и уязвимостта

- Потребителския достъп до акаунт и криптографията могат да защитят системите за файлове и данни.
- Защитните стени за сега са от най-честите системи за превенция от гледна точка на сигурността на мрежата, тъй като те могат (ако правилно са конфигурирани) да предпазят достъпа до вътрешните мрежови услуги, както и да блокират някои видове атаки чрез филтриране на пакети. Защитните стени могат да бъдат както хардуерни така и на софтуерна основа.
- Системите за откриване на проникване (IDS) са предназначени за откриване на мрежови атаки.

Днес, компютърната сигурност се състои главно от „превантивни“ мерки, като защитните стени.


https://www
Bad traffic
Internet
Firewall
Firewall blocks bad traffic
Private network