Тема 11

Мобилна сигурност

Увод

- В наши дни традиционните десктоп компютри вече не са доминиращи сред потребителите. Според https://www.statista.com/statistics/610271/worldwide-personal-computers-installed-base/ за 2019 година активно се използват около 1.4 млрд. компютри.
- Според същия сайт за 2019 година мобилните устройства в света са около 13 млрд.
- Тенденциите показват, че ролята на мобилните устройства в нашия живот ще се засилва и в близко бъдеще във всеки един аспект от живота ни ще бъде зависим от мобилни устройства.
- По тази причина сигурността и по отношение на този вид устройства е критично важна.
- Обект на внимание е сигурността на ниво операционна система, на ниво мобилно приложение и на ниво потребител.

. . .

- Наблюдава се и специфично рисково поведение от страна на потребителите на мобилни устройства
- Така например някои проучвания показват, че потребителите на смартфони са по-податливи на искане да предоставят лична информация през устройствата си (https://tech.hindustantimes.com/tech/news/smartphone-users-more-likely-to-reveal-personal-info-online-story-kLq0b6fhB72D2RjSURt6oL.html)
- Авторите обясняват това поведение така:

„Тъй като нашите смартфони са с нас през цялото време и изпълняват толкова много жизненоважни функции в живота ни, те често служат като„ биберон/залъгалки за възрастни “, които носят чувство на комфорт на собствениците си»

- И вследствие : «По същия начин, когато пишем на телефоните си, сме склонни да чувстваме, че се намираме в удобна „безопасна зона“. В резултат на това ние сме по-склонни да се отворим за себе си»

Приложения и услуги за мобилни устройства

Днес чрез мобилни устройства са достъпни множество онлайн и офлайн услуги

- Банкиране;
- Пазаруване;
- Съобщения;
- Административни услуги (държавни, общински - няма се предвид само у нас);
- Обучение;
- Развлечение;
- Споделяне на … / социални медии
- Мониторинг (видеонаблюдение, околна среда, здравен статус и др.);
- Други.

Видове мобилни устройства

- Мобилни компютри – лаптопи, таблети, Mini PC, PDA, др.
- Смартфони
- У-ва с два екрана – набират популярност, м/у таблет и смартфон
- Игрови конзоли ? (защото предлагат социални медии, интернет браузър, онлайн игри и филми)
- Wearable – смартчасовници, очила
- Цифрова навигация
- Е-книги

Характеристики на мобилните устройства (типични за 2020г.)

Форм фактор: Bar - малък

Процесор: многоядрен

ОП: 4+ GB

Вторична памет: вградена (microchip ROM) + слот + cloud

Свързаност:

- GPS
- Cellular Network - 3G, 4G, 5G
- WiFi
- NFC

Сензори:

- Accelerometer
- Gyroscope
- Ambient Light
- Compass
- Barometer
- Fingerprint sensor

Други

- Захранване - батерия
- Аксесоари – USB свързани
- Камери – 1+

Основни характеристики на мобилната сигурност (МС)

- Неделима част от другите видове сигурност
- Засяга всеки
- Изисква обучение и на потребители с ниска дигитална култура
- Високо динамична
- Висок риск (кражба на лични данни, проследяване, шпионаж видео и аудио)
- Заплахите се увеличават много бързо и стават все по-зловредни

Мобилни приложения

- Мобилен уеб – мобилни версии или адаптивни сайтове
- Нейтив - за конкретна Мобилна ОС, инсталирани
- Хибридни - за конкретна Мобилна ОС, инсталирани, но са създават с Уеб технологии, и най-актуалните Progressive Web App

Мобилни операционни системи

- **Android**
- **iOS**
- **Microsoft** – Mobile и Phone (вече не се поддържат), но продължават да се използват макар и ограничено
- **KaiOS** - в ранен етап на развитие на базата на Linux, за устройства от нисък клас с ограничени услуги без сензорни екрани
- **Други**

Android security features*

- App sandbox – на всяко приложение се присвоява уникален идентификатор и то се стартира като отделен процес
- App signing – за да се инсталира приложението то трябва да бъде цифрово подписано от разработчика
- Authentication – за автентикация се използва сензор за пръстов отпечатък, лицево разпознаване, ПИН или Патърн, първоначално се генерира уникален идентификатор на потребителя, а след това се използва за генериране на ключ съхраняван в специален склад
- Encryption – използва се както симетрично така и асиметрично криптиране вкл. и за вътрешна комуникация
- Keystore - на хардуерно ниво
- …

* https://source.android.com/security/features

Apple Platform Security*

- Вградени механизми на хардуерно ниво – напр. чип за AES криптиране на файловете при четене и запис
- На ниво операционна система – Secure boot, software updates, ОС ъпгрейд без възможност за даунгрейд
- Biometric
- Encryption
- App sandbox
- Сигурни услуги - iCloud, Apple Pay, iMessage, FaceTime

* https://support.apple.com/guide/security/welcome/web

Активи обект на мобилна защита

- **Устройства**
- **Мобилни приложения**
- **Данни**, в т.ч. лични, фирмени, банкови, пароли и др.
- **Сертификати –** импорт/експорт винаги с парола
- **Изображения, аудио и видео записи**
- **Контакти**
- **Съобщения** в т.ч. SMS, email, социалните медии

Вектори на атака (Attack Vector)

- Attack Vector е метод или техника, която хакерът използва, за да получи достъп до устройство, за да внесе зловреден код/инфектира устройството.
- Мобилни приложения – както заразени след инсталация, така и умишлено вмъкнат код от разработчика
- Мрежови атаки – най-често по незащитени WiFi мрежи
- Дупки в сигурността в МОС или „рутнати“ устройства

Видове заплахи за мобилната сигурност (https://www.lookout.com/know-your-mobile/what-is-a-mobile-threat)

Мобилно приложение

- **Malware-** софтуер, който извършва зловредни действия на устройството
- **Ransomware –** може да промени PIN и криптира файловете за откуп (напр. DoubleLocker)
- **Spyware** - софтуер, който събира чувствителна информация, която може да се използва за кражба на самоличност или финансови измами
- **Privacy Threats** – софтуер, който не може да бъде класифициран като зловреден, но може да събира чувствителна информация
- **Vulnerable Applications –** не добре защитени приложения, които могат да бъдат използвани като врата за пробив

Видове заплахи за мобилната сигурност (https://www.lookout.com/know-your-mobile/what-is-a-mobile-threat)

Уеб-базирани

- **Phishing Scams**
- **Drive-By Downloads** – автоматично изтегляне на софтуер при посещаване на уеб сайт
- **Browser exploits** – уязвимости в браузъра или в помощни програми като Flash player, PDF reader или image viewer

Мрежови

- **Network exploits** – уязвимост в ОС или приложение при работа в мрежа - клетъчна или безжична
- **Wi-Fi Sniffing** – прихващане на данни
- **Botnets**

Физически

- **Кражба и изгубване**
- **Ремонт**
- **Безконтактни услуги** – разплащане, отключване/заключване

Най-разпространения малуер за Android за 2020 г.

- FakeInst
- OpFake
- SNDApps
- Boxer
- GinMaster
- VDLoader
- FakeDolphin
- KungFu
- Basebridge
- JIFake

Признаци за заразено устройство

- Проверка за „рутнато“ устройство – ако потребителя не е предприемал такова действие
- По-бързо изтощаване на батерията – ако в последните дни времето за работа значително намалява
- Често крашване на приложения – актуализация
- Установяване на непознати приложения
- Увеличаване на поп-ъп съобщенията/рекламите
- Увеличаване на месечната такса
- Бързо изчерпване на мобилни данни на максимална скорост

Човешки фактор

- **Информираност**
  - през официалните канали на платформите
  - специализирани сайтове напр. https://www.infosecurity-magazine.com/mobile-security/
  - други доверени източници
- **Мерки**
  - физическа защита
  - антивирусен софтуер
  - обучение
  - използване само на проверени приложения и премахване на рядко използвани
  - актуализации
  - не „рутване“ на устройствата
  - настройки – различни за различните ОС и версии
  - мониторинг
  - бакъп
  - използване на virtual private network (VPN) в бизнес среда

BYOD

- **Bring Your Own Device**
- Политика на компании и образователни институции да насърчават служители да използват собствени устройства на работното място
- Устройствата се използват за достъп и работят с корпоративните данни и системи
- Особено се увеличава в пандемията и необходимостта от работа от вкъщи
- Заплахите за сигурността са много големи, тъй като:

- ❑ съществува голям риск от теч на корпоративни данни
- ❑ на устройствата има инсталиран по-голям брой и несигурен софтуер, вкл. пиратски
- ❑ остарели ОС, не настроени правилно, липсващи актуализации
- ❑ устройствата се използват от много хора
- ❑ съхраняват се данни като се смесват с такива от личния живот

Mobile device management (корпоративно ниво)

- Администриране на мобилни устройства
- Реализира се чрез използване на специален софтуер
- Представлява комбинация от приложения, настройки, сертификати, политики за сигурност и сървър(компонент)/клауд
- Донякъде аналогия с Windows Update
- На мобилните устройства се инсталира клиентска част, която може да получи команди от сървър
- Администратор централизирано може да подаде команди за актуализиране или прилагане на настройки на всяко устройство с инсталиран клиент
- Може отдалечено да се изтриват данни или цялото устройство, да се заключи устройството и др.
- Примери: **Jamf Pro**, **Scalefusion, Sophos Mobile, Hexnode MDM**

IoT security

- Електронни и механични устройства, които имат вградена електроника, която позволява тези устройства да се свързват към Интернет
- Тези устройства могат да събират и да предават данни
- Разпространяват се много бързо сред всички групи хора, бизнес, личен живот
- Считат се за основа на четвъртата индустриална революция
- Те също са изложени на риск, най-известен пример е Mirai Botnet.
- Устройства:

- Автомобили -Jeep Hack
- Умни телевизори – FBI записване на глас, 2018 г. ADB.Miner копаене на криптовалута
- Умни охранителни камери Xiaomi и Amazon's Ring Video Doorbell Pro
- Факс машини
- Кафеавтомати и кафемашини – 2019 Avast
- Рутери

Още на https://cisomag.eccouncil.org/10-iot-security-incidents-that-make-you-feel-less-secure/ и https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities/

Мобилна сигурност – добри практики

- Да се използват различни устройства за лични и за бизнес нужди
- Да се използват различни акаунти или профили за лични и бизнес нужди включително за данните и приложенията
- Ако е възможно да се използва двуфакторна автентикация – мобилните устройства са особено подходящи за това напр. чрез SMS
- При изгубване или кражба на устройство да се уведомят Контактите и/или IT отдела, да се използват функции за търсене (Find My Device), отдалечено заключване и изтриване (Remote lock & wipe)
- Когато не се използват да се деактивират Bluetooth и Wi-Fi;
- Да се направи застраховка Кибер …. сигурност/отговорност - най-вече за бизнес нужди, цена от няколко стотин лева

Мобилна сигурност – добри практики

На мобилни устройства използвани за бизнес нужди да се:

- инсталират и използват само лицензирани приложения;
- използват само за работа и лично;
- настроят на най-високото ниво на сигурност;
- прави бакъп на повече от едно място;
- използва VPN;
- използват Password Manager-и;
- променят много по-често паролите и ПИН – препоръчително е веднъж на седмица;

Заключение

- Мобилните устройства вече са неизменна част от нашия живот.
- Информацията която се съхранява на тях е сравнима по значение с тази на настолните устройства, а в някои случаи и много по важна за нас.
- Необходимо е да се прилагат мерки за защита дори в по-голяма степен, тъй като те лесно могат да бъдат откраднати или изгубени.

Практически упражнения

- В рамките на един учебен час потърсете в Интернет пространството информация за разглежданите в темата понятия, дефиниции и аспекти. Търсенето може да направите и на чужди езици, които владеете.
- Анализирайте намерената информация и я сравнете с поднесената тук.
- Проучете мобилните си устройства – каква информация съхранявате на тях, как са защитени и достатъчни ли са мерките за защита.