Ældre Sagen
Willi Nielsen

Lokalafdeling Bov, IT

Mobil: (+45) 2030 0104 e-mail: willi.6340@outlook.com

Sikkerhed, virus-begreber, februar, 2015.

1. Begreber for sikkerhed på en tablet (og ligeledes for Smartphones).

Sikkerhed på "mobile enheder" (her defineret som Tablets og Smartphones) omfatter disse hovedemner:

a) Antivirus, Spyware, Malware
b) Phishing
c) Firewall

Ad a) Antivirus, Spyware, Malware.
På en "mobilenhed" afvikles der **ikke** programmer (programmer afvikles på en PC), men **apps** (applications).
Et **program** kan interagere med andre programmer og dermed "sprede en virus".

En app har ikke "adgang" til en anden app, og kan derfor ikke sprede en evt. virus.
En app

- kan ikke "selv replikere"
- Kan ikke komme ud med en virus (kan ikke sprede en virus)
- Kan ikke eksekvere (udføre) en såkaldt exe.fil, som er den metode, hvorved en virus spredes på en "normal" PC,

Derfor er der **ikke umiddelbart behov** for en antivirus-app på en tablet (se dog nedenfor under Windows 8.1).

2. Definition af og karakteristika ved Virus / Malware.

Info hentet fra "Trend Micro" (Søgte på "replikere sig selv")
http://docs.trendmicro.com/all/smb/wfbs-services/Server/Dell/v3.6/da/docs/WebHelp/_WFBS-SVC/C01-ProductOverview/UnderstandingThreats.htm

Ordet Malware er en sammentrækning af de engelske ord *malicious software* (på dansk: "ondsindet programkode").

Overordnet definition af "Virus / malware"

- Computervirus/-malware er et program –
  - **et eksekverbart kodestykke**,
  - der har en særlig evne til **at replikere sig selv** (dvs. at sprede en virus).

Karakteristika ved "Virus / malware"

- Virus / malware kan føje sig selv til stort set alle typer eksekverbare filer og spredes som filer, der kopieres og sendes fra person til person.
- Ud over at kunne replikere sig selv kan computervirus / -malware have en anden ting tilfælles:
  - en skadesrutine, som leverer virussens skadelige data.
  - Mens visse skadelige data kun kan vise meddelelser eller billeder,
  - kan andre ødelægge filer, omformatere harddisken eller forårsage andre skader.

3. Hvordan kommer en virus ind til din enhed.

Farlig kode kan komme ind i dit system og forvolde skade ad mange forskellige kanaler.
Mobil kode kan selv komme rundt - den behøver blot en åben pipeline - og det er derfor, bredbåndsforbindelser så ofte bliver ofre for den.
Virus kommer rundt som "blinde passagerer".
De to hyppigste veje ind til pc'en for denne type virus eller inficeret kode er

- gennem overførsler fra Websteder,
- via e-mails,
- i vedhæftede filer i e-mails.

Willi Nielsen Mobil: (+45) 2030 0104 e-mail: willi.6340@outlook.com

Når en inficeret fil åbnes, eksekveres den integrerede virus.
Ofte er brugere ikke klar over, at dette foregår i baggrunden.
Malware kan replikere sig selv inden for én computer, men den ikke kan sprede sig selv fra computer til computer uden hjælp.
For at kunne inficere andre maskiner skal den

- sendes videre i et program,
- sendes videre via en e-mail-fil eller en vedhæftet fil,
- en inficeret DVD eller andre "ikke-permanente medier" (f.eks. en USB-stikker).

4. Oversigt af "typer af Virus".

a) **Malware:**

- Malware er et fællesbegreb for software, der er udviklet til at infiltrere eller beskadige et computersystem, uden ejerens samtykke.

b) **Orme:**

- En **orm** er et program, som faktisk kan formere sig uden brugermedvirken. En orm er ikke teknisk set en "virus", fordi den kan reproducere sig selv - af sig selv. Et godt eksempel herpå er e-mail-ormen ILOVEYOU, som automatisk e-mailede sig selv til alle i modtagerens adressekartotek. En orm kan sprede sig til hundredtusindvis af maskiner meget hurtigt via de lokale netværk og Internettet.
- En computerorm er et selvstændigt program (eller flere programmer), der kan sprede funktionsdygtige kopier af sig selv eller dele af sig selv til andre computersystemer.
- Spredningen sker som regel via netværksforbindelser eller vedhæftede filer i e-mail.
- I modsætning til virus/malware behøver orme ikke at vedhæfte sig selv til værtsprogrammer.

c) **Trojanske heste:**

- En trojansk hest er et skadeligt program, der udgiver sig for at være et harmløst program, f.eks. en pauseskærm, et spil eller en anden type hjælpeprogram..
- I modsætning til virus/malware kan trojanske heste **ikke** replikere sig selv. De er udelukkende destruktive.
- Det replikerer ikke sig selv som en virus, kopierer ikke sig selv som en orm.
- Det spredes normalt pr. e-mail eller via Weboverførsler.
- Et program, der hævder at fjerne virus/malware fra computeren, når det rent faktisk tilfører computeren virus/malware, er et eksempel på en trojansk hest.

d) **Bagdør:**

- En bagdør er en metode til at omgå normal godkendelse, opnå fjernadgang til en computer, og/eller opnå adgang til oplysninger, uden at det bliver opdaget.

e) **Rootkit:**

- En rootkit er et sæt programmer, der er udviklet til at beskadige brugernes legitime styring af et operativsystem.
- En rootkit skjuler som regel, at den er installeret, og forsøger at forhindre, at den fjernes, ved hjælp af en del af standardsystemsikkerheden.

f) **Makrovirus:**

- En makrovirus er programspecifik.
- Virussen findes i filer til programmer, f.eks. Microsoft Word (.doc) og Microsoft Excel (.xls).
- De kan derfor registreres i filer med filtypenavne i programmer, hvor makroer normalt kan benyttes, f.eks. .doc, .xls og .ppt.
- En makrovirus bevæger sig mellem datafiler i programmet og kan efterhånden inficere hundredvis af filer, hvis den ikke bliver opdaget.

5. Oversigt af "Grayware / Spyware".

Grayware er et program, der udfører uventede eller uautoriserede handlinger.

Willi Nielsen Mobil: (+45) 2030 0104 e-mail: willi.6340@outlook.com

Det er et overordnet begreb, der bruges til at henvise til

- spyware,
- adware,
- dialers,
- programmer med vittige filer,
- fjernadgangsværktøjer

Afhængigt af typen, kan den medføre replikering eller ikke-replikering af skadelig kode.

a) **Spyware:**
- Spyware er computersoftware, der installeres på en computer uden brugerens samtykke eller viden, og det indsamler og sender personlige oplysninger.

b) **Adware:**
- Adware, eller reklameunderstøttede programmer, er programpakker, der automatisk afspiller, viser eller henter reklamer til en computer, når softwaren er installeret på den, eller mens programmet bruges.

c) **Keylogger:**
- En keylogger er et computerprogram, der logfører alle brugerens tastetryk. Disse oplysninger kan derefter hentes af en hacker og bruges til personlige formål.

d) **Dialers:**
- Dialers er nødvendige for at oprette forbindelse til internettet ved forbindelser uden bredbånd.
- Skadelige dialers er udviklet til at oprette forbindelse via numre til særtakst i stedet for at oprette direkte forbindelse til internetudbyderen.
- Udbydere af disse skadelige dialers tager selv de ekstra penge.
- Dialers kan også bruges til at sende personlige oplysninger og hente skadelig software.

e) **Hackingværktøj:**
- Et hackingværktøj er et program, eller flere programmer, der er udviklet til at hjælpe hackere.

f) **Robot:**
- En robot er et program, der fungerer som en agent for en bruger eller et andet program, eller som simulerer en menneskelig aktivitet.
- Når der er kørt en robot, kan den replikere, komprimere og distribuere kopier af sig selv.
- Robotter kan bruges til at koordinere et automatisk angreb på netværkscomputere.

6. Firewall.

Firewallen og netværkets virusmønsterfil er sammen om at identificere og blokere netværksvirus.

Indtrængen:
- Indtrængen betyder, at der opnås adgang til et netværk eller en computer enten med magt eller uden tilladelse.
- Det kan også betyde, at netværks- eller computersikkerheden tilsidesættes.
- Falske adgangspunkter, der også kendes som Evil Twin, er et begreb i forbindelse med et rogue-Wi-Fi-adgangspunkt, der lader til at være lovligt og tilbudt på stedet, men som rent faktisk er konfigureret af en hacker for at smuglytte til trådløs kommunikation.