

IKT SIKKERHET

Sigurd Skauvik MOUS

Først vil jeg forklare litt hva Malware er og forskjellen på virus og annet ondsinnet programvare.

Malware er samle betegnelsen på virus, worm, spyware, adware og trojan.

- **Virus**
Et program som kan installere seg selv på en maskin. Et virus kommer ikke over nettverket selv uten at du åpner en mail e.l. Når et virus er installert, viruset ødelegger eller kompromiserer systemet på en eller annen måte
- **Worm**
En orm kan spre seg over nettverket automatisk uten hjelp av et program. Ormer varierer veldig i hvor mye ødeleggelser den kan gjøre. Noen bare bruker opp båndbredde, andre kan utsette systemet helt.
- **Trojan Horse**
En Trojan er et program som presenterer seg som et fint program, men er skrevet for å skade systemet. I ulikhet med virus og ormer, så kopierer en Trojan segt ikke selv eller installerer seg selv. Brukeren må selv åpne programmet.
- **Spyware**
Spyware er en type privat-invaderende software som samler og lagrer informasjon om hva brukeren gjør, ofte for markeds undersøkelser. Typisk blir spyware installert når brukeren installerer et gratis verktøy eller besøker en nettside og har lav sikkerhet på nettleseren. Den lagrer ofte web-sider du bruker. Mer sjelden, noe spyware, som keyloggers (som lagrer hvert tastetrykk) kan bli installert av en tredjepart og brukt til å samle personlig informasjon.
- **Adware**
Adware ligner på spyware og er ofte installert i tillegg. Målet for Adware er å vise reklame til brukeren i form av popup vinduer eller web-sider. Adware kan også laste ned Spyware.

NOEN TOMMELFINGER REGLER FOR Å HOLDE DEG SIKKER:

1. Hold windows oppdatert
2. Bruk antivirus program
3. Ha aktiv brannmur
4. Hold også programmene dine oppdatert

SIKKERHET – SMARTCARD

Windows 7 støtter bruk av smartkort. Et smartkort er på størrelsen som et bankkort, inneholder en chip med et sertifikat som unikt identifiserer brukeren. Å sette inn et smartkort er nok til å bekrefte brukern. Typisk må brukeren også bruke et passord eller en PIN for å bevise at brukeren ikke bruker noen andre sitt smartkort. Når du bruker både passord og et smartkort kalles det *Multifactor Authentication* på engelsk.

Biometrics er en annen populær form for authentication. I dag er den mest populære formen for biometrics fingeravtrykks leser.

SIKKERHET – CREDENTIALS

Legitimasjon

Windows legger automatisk til Credentials når en bruker kobler seg til en delt mappe til Credential manager. Men, du vil kanskje legge til ett brukernavn og passord manuelt. For å gjøre det følg disse punktene:

1. Klikk *start og kontrollpanel*
2. Klikk *brukere og grupper*
3. Til venstre, klikk *manage your credentials*
4. Klikk *add new windows credential*
5. I *internett eller nettverk* boksen, skriv nettverksnavnet.
6. I *brukernavn og passord* boksene, skriv inn dine brukers Credentials.s

AUTHENTICATION OG AUTHORIZATION

Disse to prosessene er ganske like, og det kan være greit å vite forskjellen på disse.

Authentication

Direkte oversatt: bekreftelse.

Dette er prosessen for å identifisere brukeren, i hjemmemiljø. Authentication er ofte så enkelt som å klikke på brukernavnet ved windows 7 velkommen skjermen. Men i et foretaksmiljø, nesten alle bekreftelses forespørsler pålegger brukere å bekrefte både et brukernavn (for å identifisere seg selv) og et passord (for å bevise at de virkelig den de sier de er).

Authorization

Direkte oversatt: Fullmakt, bemyndige

Dette er prosessen av validering gjennom verifikasjon av et passord eller andre legitimeringer som f.eks et sertifikat eller smart-kort, for å se om brukeren er den han/hun sier den er.s

sigurd skauvik