**Stuxnet:**

Cyber trusler har vært et økende problem helt siden internetts eksistens , og det bare fortsetter å spre seg fra dag til dag . Det er i all hovedsak myndighetene og de store bedriftene som er hardest rammet av disse truslene. Cybertruslene sprer seg hovedsakelig gjennom internett og er en type internettkonflikt som involverer angrep på blant annet politiske informasjonssystemer. Men hva er hovedårsaken til det? Vell, man antar at disse truslene var laget av svindlere eller hackere som egentlig var ute etter penger, og formålet med disse truslene var hovedsakelig sabotasje eller spionasje av et system. Hvis man ble utsatt for slike cyber- angrep kan f.eks. dataen i systemet modifiseres utilsiktet eller stjeles, og i verste fall kan hele systemet deaktiveres eller forstyrres. Dette er som sagt et økende problem, og det påvirker ikke bare store bedrifter og selskaper, men det kan også påvirke et helt land. For i 2010 var det en historisk hendelse som inntok i Iran. De var nemlig utsatt for et dataangrep kalt Stuxnet, men hva var dette angrepet egentlig?

Stuxnet var en orm som ble utviklet av den amerikanske regjeringen i samarbeid med Israel. Denne ormen var utviklet hovedsakelig for Natanz atomkraftverk i Iran, fordi de fryktet at de produserte atomvåpen som kunne utløse eller medføre en krig. Dette ble ansett som en trussel av USA og Israel. Dette ble først juni 2010 oppdaget av et iransk firma som sendte en epost til det russiske sikkerhetsfirmaet VirusBlokAda om mistanke av muligens funn av et datavirus. Deretter analyserte sikkerhetsfirmaet disse infiserte maskinene og besluttet seg fram til at dette var en orm, og varslet dette videre til resten av sikkerhetsindustrien, som ble over tid kjent for resten verden .

Stuxnet ormen spredde seg uten at maskinen var tilkoblet til internett, og du tenker kanskje : «Hæ, hvordan er det mulig?» Det magiske svaret på det var at den ble spredd via USB-pinner og en exploit av LNK fil formatet som lot ormen bryte seg inn i nettverk eller maskiner uten at de var tilkoblet til internett. Den infiserte hovedsakelig maskiner som kjørte Siemens SCADA systemer, men også Windows. Når en maskin ble infisert, forplantet Stuxnet seg i det nettverket maskinene var koblet til, og infiserte absolutt alle maskinene på det nettverket. Denne ormen har «Peer -to- Peer» P2P mekanismer med noen kjente sårbarheter og inkluderte i tillegg fire «Zero-day - exploits» . Denne ormen var hovedsakelig ute etter maskinene som kjørte SCADA , og hvis den infiserte maskiner utenom det som f.eks. Windows maskinene, gjorde den egentlig ingenting. Hvis den detekterte SCADA -maskinene, infiserte ormen dem ved å ta i bruk en ukjent og u -opprettet sårbarhet i WinCC kontrollerprogramvaren. Deretter spredde ormen seg videre til PLC-en i Siemens-systemet via en feil i WinCC databasen. Siden hoved administrator passordet var felles på alle SCADA-maskinene, opprettet Stuxnet en feil i systemets klient som gjorde at hvis man prøvde å endre på disse passordene, så kræsjet klienten. Men heldigvis for ormens utviklerne visste ikke Siemens om denne feilen, som betød at passordet forble uendret som Stuxnet hadde i sine hender, og hardkodet. Denne ormen påvirket ikke bare Iran, men ble også oppdaget i en del naboland som Pakistan, India ,Taiwan , Indonesia . Stuxnet infiserte over 200 000 datamaskiner, og ormen anses som et av historiens verste cyber-angrep gjennom tidene fordi denne var utviklet for å skade et helt system bare for å forhindre et land fra å lage atomvåpen.

Etter at ormen forårsaket en sabotasje mot det iranske atomsystemet , skapte dette en del spekulasjoner , og spørsmålet om hvor alvorlig de fremtidige cyber- truslene kan være for den fysiske verden ble et viktig grunnlag for debatten om hvordan et system skulle sikres mot disse truslene i fremtiden. Stuxnet hendelsene som inntok i Iran for 12 år siden, bringer folk inn i et nytt perspektiv av cyber-trusler som ikke bare påvirker den digitale verden , men også den fysiske.

Jeg tror personlig at dette vil være et økende problem i fremtiden og etter hendelsene som USA har forårsaket mot Iran, burde vi fremdeles forberede oss på andre type virus og ormer som kan være mye alvorligere enn det Stuxnet var. Hvis dette forblir til å bli et økende problem så kan det bli mer tungvint og komplisert å håndtere og stoppe disse truslene. Hvis dette vedvarer, vil dette ikke bare påvirke verden fysisk, men også for oss som er vant til å bruke datamaskiner i hverdagen. Dette vil også påvirke store bedrifter som lagrer så si all dataen sin inn i et system, for hvis de blir utsatt av et alvorlig virus kan systemet deres bli ødelagt. Og hvis et system er sabotert vil dette gå utover et selskap som kan medføre til at de går konkurs hvis det blir vanskelig å stoppe viruset de er infisert med, avhengig av alvorlighet. Verden er i en epoke hvor teknologi spiller en viktig rolle der datavirus har blitt utviklet av svindlere til å skade maskinene våre. Dette har medført store konsekvenser for i all hovedsak for stedene der system er dominerende, som har dataen sin lagret i et system som er lokalisert for det meste digitalt, med andre ord på maskinene deres. Ja det er utviklet antivirusprogram for å forhindre virus fra å infisere maskinene våre, men er det nok? En eller annen gang vil jeg frykte at disse antivirusprogrammene vil være udugelige mot disse truslene, ettersom de vokser seg til å bli flere og mer alvorlige. Det vil ikke være sikkert å benytte seg av datamaskinene lenger, så hva skjer da og hvor skal dataene lagres ?

**Skriv et kort essay (en side eller to) om Stuxnet**

**• Hva ble angrepet**

**• Hvem stod bak, og hvorfor**

**• Lag ditt eget skrekkscenario for fremtiden**

**• Individuell innlevering. Frist 7. april, detaljer kommer som kunngjøring på Canvas**

**KILDER:**

* Østby, Bengt (Norge) . «TK2100\_04\_Kinetisk.pdf» .Oslo, Oslo ,slide(19, 22)
* <https://en.wikipedia.org/wiki/Stuxnet>
* <https://www.britannica.com/technology/Stuxnet>
* <https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-stuxnet.html>