Trusselen fra cyberspace

Cyberangrep øker i omfang verden over. Norge er et av verdens mest digitaliserte land og dermed spesielt utsatt, men dette blir i stor grad oversett av politikere og næringslivsledere.

På samme måte som luftfart endret verden på begynnelsen av 1900-tallet endrer informasjonsteknologi verden i dag. Cyberangrep begynner å bli vanlig, og Norge er spesielt utsatt, men utfordringen blir i stor grad oversett av politikere og næringslivsledere, skriver artikkelforfatterne.
FOTO: DANIEL NORDBY / FORSVARET

Niels Nagelhus Schia
@nielsschia
seniorforsker, NUPI

Lilly Pijnenburg Muller
forsker, NUPI

Publisert 21.12.2016, kl. 13:25

kronikk

Da Barack Obama overtok nøklene til Det hvite hus fra George W. Bush i 2009, fikk han samtidig et råd om å videreføre et topphemmelig sikkerhetsprogram. Dette programmet ble kalt Olympic Games, men er kjent som Stuxnet, og kalles gjerne verdens første cybervåpen.

Åtte år senere har USA selv vært offer for flere cyberangrep og angrepene øker i antall og omfang verden over.

Nylig anklaget Obama Russland for å ha hacket e-postserver til Demokratene (DNC), og påvirket valget av USAs neste president. Når Obama overleverer nøklene til Donald Trump om en måned, står cyberangrep derfor høyt på agendaen i USA og globalt.

> *Les også:* Russerne ber USA legge fram bevis for hacking

Tre kategorier

Et cyberangrep er et angrep som skjer enten via digitale nettverk eller er rettet mot digitale nettverk. Norge er et av verdens mest digitaliserte land og dermed spesielt utsatt. Hvis den politiske motivasjonen er til stede, kan angrep også skje her.

Cyberangrep kan deles opp i tre hovedkategorier:

1. For det første har vi den type angrep som er rettet mot å ødelegge fysiske installasjoner som å kutte kabler eller ødelegge basestasjoner for å sette kritisk infrastruktur ut av spill.
2. I den andre kategorien sorteres den type angrep som utføres gjennom dataskadevare, virus og dataormer som for eksempel Stuxnetormen. Alex Gibneys film «Zero Days», som i disse dager vises på NRK, nøster opp i historien om Stuxnet og denne typen angrep.
3. I den tredje kategorien finner vi angrep som bruker digitale nettverk som verktøy for propagandakampanjer og til å spre villedende informasjon.

Den første og tredje kategorien innebærer egentlig ikke noe nytt i denne sammenheng. Ødeleggelse av infrastruktur, samt propaganda og informasjonskampanjer, kjenner vi fra historien. Men angrep via digital skadevare som virus og dataormer, det vil si den andre kategorien, gir nye muligheter til å skjule angriperen og til lettere å nå nye typer mål.

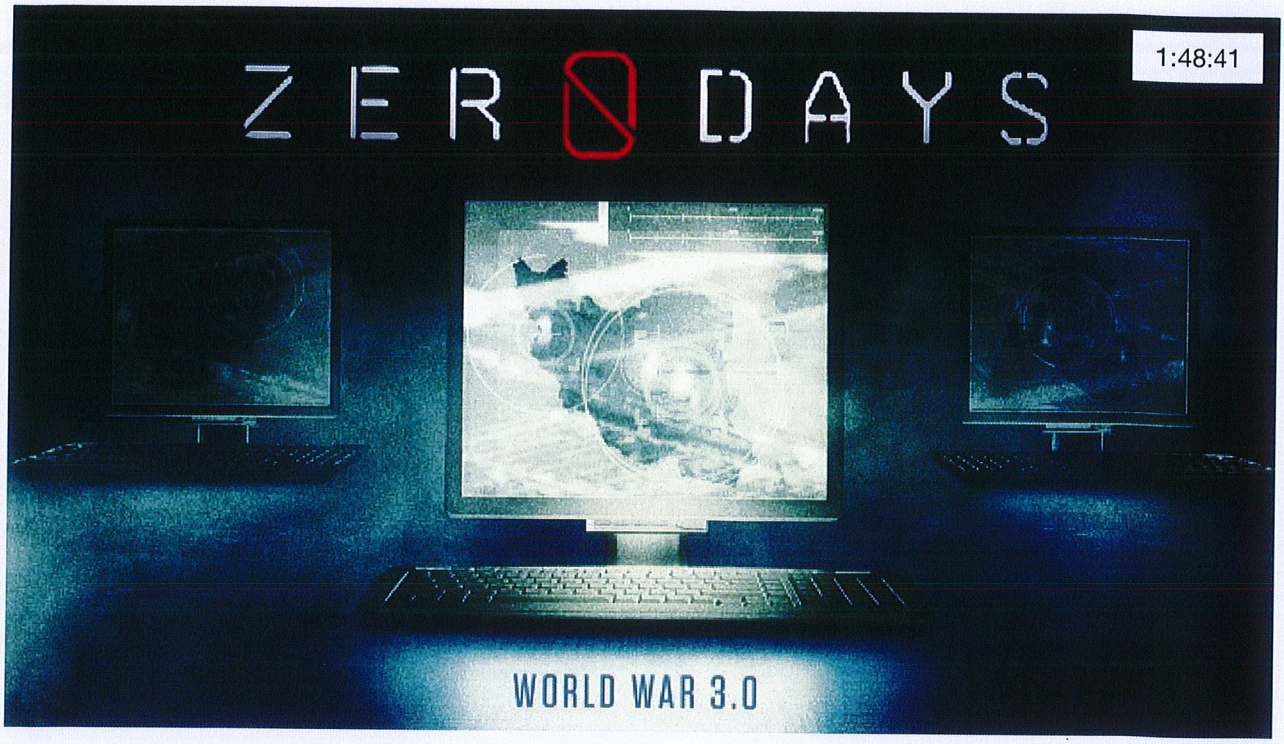
Zero Days

Filmen «Zero Days» formidler hvordan digitale sårbarheter kan utnyttes gjennom cyberangrep for å skape politisk press i betente forhandlingssituasjoner og konfliktsituasjoner, eller for å ødelegge et lands kritiske infrastruktur.

Filmens handler om Stuxnet, en sofistikert programvare eller dataorm som ble påbegynt i 2005. Mange mener at Stuxnet representerte noe helt nytt da den ble tatt i bruk i 2007.

Tidligere hadde man sett eksempler på skadevare og virus som ble brukt for å ta kontroll over andre datamaskiner og til å stjele digital informasjon.

Se filmen her:



Gjennom digitale nettverk skadet Stuxnet fysiske installasjoner i Natanz i Iran. Sentrifuger som ble brukt til anriking av uran ble programmert til å eksplodere uten å avsløre programvaren. Disse hendelsene ble igjen brukt til å påvirke politiske prosesser.

Digital sårbarhet utnyttes

Tittelen på filmen, «Zero Days», spiller på et teknisk begrep som referer til hvor mange dager en programvareingeniør har til å reparere ett «hull», eller ukjent sårbarheter i koder til digitale nettverk etter at de har blitt oppdaget og utnyttet. Angrepet ble oppdaget i 2010, men hadde da allerede rukket å forsinke Irans kjernevåpenproduksjon betraktelig i en periode på tre år.

Filmen er interessant utover hvordan den forteller historien om sårbarheter i Irans kjernevåpenproduksjon:

For det første fordi den formidler hvordan digitale sårbarheter kan utnyttes gjennom cyberangrep. For det andre fordi den forteller hvordan slike angrep kan brukes til å skape politisk press i betente forhandlingssituasjoner og konfliktsituasjoner. Og for det tredje

viser den også hvordan kritisk nasjonal infrastruktur blir stadig mer utsatt.

> *På samme måte som luftfart endret verden på begynnelsen av 1900-tallet endrer informasjonsteknologi verden i dag.*

På samme måte som luftfart endret verden på begynnelsen av 1900-tallet endrer informasjonsteknologi verden i dag. Frankrikes forsvarsminister Jean-Yves Le Drian sammenlignet nylig betydningen av hacking og cyberangrep med betydningen av de første flyene som ble brukt i konflikter under første og andre verdenskrig da han tidligere i desember lanserte Frankrikes nye avdeling for cyberkrig.

Stuxnet representerte på mange måter startskuddet for et internasjonalt kappløp der hacking og cyberangrep ikke bare brukes til etterretning og rekognosering, men også som ledd i offensive angrep. Men Stuxnet er langt ifra det eneste slike angrepet vi kjenner.

På lille julaften 2015 ble 230 000 innbyggere i Ukraina strømløse på grunn av et cyberangrep mot strømnettet i landet. Ukraina beskyldte Russland for å stå bak. Nylig har vi kunnet lese om hacking av e-postserveren til de demokratiske partiet i USA og hvordan dette forstyrret den amerikanske valgkampen.

› *Les:* Obama beordrer full gjennomgang av mulig valg-hacking

David E. Sanger beskrev nylig i New York Times hacking i denne sammenheng som «the perfect weapon»: Det er billig, vanskelig å forutse og oppdage, og vanskelig å spore.

Det første cyberangrepet

Det som ofte beskrives som det første cyberangrepet mellom stater blir kalt Moonlight Maze (1996-1998). Der stjal hackere tusenvis av sensitive dokumenter fra amerikanske offentlige institusjoner og det amerikanske forsvaret. USA har beskyldt Russland for å stå bak dette angrepet.

Siden Moonlight Maze har listen over cyberangrep vokst. I tillegg til Stuxnet og Ukraina, nevnes også ofte cyberangrepet på Estland i 2007, som satte nettsidene til parlamentet, departementer, banker og store medieselskaper ut av spill.

Georgia opplevde et lignende angrep året etter. Problemene med å spore angrepene gjør

at man i stor grad står igjen med beskyldninger og anklager, snarere enn håndfaste bevis. Både Georgia og Estland har pekt på Russland.

Cyberangrep er ikke kun rettet mot stater, også private selskaper er utsatte. Slike angrep blir stadig mer vanlige, og i 2014 fikk et tysk stålverk omfattende skader da hackere tok kontroll over programvare knyttet til produksjonsvirksomheten. Også dette angrepet har vært vanskelig å spore, og det er uklart hvem som stod bak og hva hensikten deres var utover å ødelegge produksjonen.

> *Økt aggresjon fra stater via cyberspace fremstår stadig mer som en ny form for geopolitisk risiko.*

Økt aggresjon fra stater via cyberspace er en voksende geopolitisk risiko. Nato har også anerkjent denne faren. Tidligere i år definerte Nato cyberspace som et selvstendig forsvarsdomene, på samme måte som land, sjø og luft.

Mange land kjemper hardt for å ligge foran

Teknologien som ligger til grunn for hacking og cyberangrep er under rask utvikling. Mange land kjemper nå hardt for å ligge foran i den teknologiske utviklingen. Ny teknologi åpner for nye typer angrep og nye former for etterretning.

> *Dagen etter at Norge vedtok å sende jagerfly til Libya i 2011 ble forsvaret utsatt for et digitalt angrep.*

Dagen etter at Norge vedtok å sende jagerfly til Libya i 2011 ble forsvaret utsatt for et digitalt angrep. Politisk motiverte digitale angrep mot norske departementer, politikere og næringsliv er likevel fortsatt en utfordring som i stor grad blir oversett av politikere og næringslivsledere.

All den tid Norge er en viktig leverandør av for eksempel energi – olje og gass – til Europa, innebærer denne nasjonale utfordringen også et element av europeisk sikkerhet.

› *Les også:* Hvem skal sitte med «atomkodene» våre?

FØLG DEBATTEN: NRK Debatt på Facebook **OG** @NRKYtring på Twitter

Publisert 21.12.2016, kl. 13:25