EMNER *Malware-virus, Hacking, Stuxnet*

Nato klar til cyberkrig: Angreb mod én er angreb mod alle

Den berømte musketer-ed blandt Natos medlemslande skal også gælde cyberangreb. Men landene er uenige om, hvordan et storstilet hackerangreb skal afværges.

Af ***Jesper Kildebogaard*** *Onsdag, 13. oktober 2010 - 13:04*

Hvis et Nato-land bliver massivt angrebet via internettet, skal resten af medlemmerne i forsvarsalliancen ikke sidde med hænderne i skødet.

Sådan lyder oplægget til et kommende Nato-topmøde i november, hvor cyberkrig efter alt at dømme vil blive ligestillet med regulær krig, så musketer-eden mellem landene også bliver taget i brug her. Det skriver Jyllands-Posten.

»Cyberangreb kan få et lands luftfartskontrol til at gå i sort, lukke bankerne, lamme offentlige myndigheder og være ødelæggende for økonomien. Med andre ord: De kan true fundamentale sikkerhedsinteresser hos de allierede,« siger Anders Fogh Rasmussen, generalsekretær for Nato, til Jyllands-Posten.

Nato fik for alvor øjnene op for truslen for cyberkrig, da Estland i 2007 blev udsat for et angreb, der lammede mange vigtige websider. Baggrunden var en politisk beslutning, der var upopulær hos det russiske mindretal i landet. Siden har diskussionen i Nato kørt på, om et cyberangreb rummer samme alvor som et angreb med krudt og kugler.

Med afklaringen og ligestillingen af digitale og analoge angreb står Nato-landene over for en ny, vigtig diskussion, nemlig om man må angribe computere i andre lande, eller skal holde sig til rent forsvar. Her er der ikke enighed mellem landene.

USA har oprustet kraftigt til cyberkrig og er klar til at slå først, mens en række europæiske lande er skeptiske over for at skulle udføre angreb mod it-systemer på fremmed grund.

En lind strøm af mindre angreb hver dag på Natos it-systemer minder i øvrigt Nato-folkene om problemet. Ifølge Anders Fogh Rasmussen er der 100 hackerangreb om dagen.

Samtidigt har den meget avancerede orm Stuxnet skabt uro verden over, da malwaren går direkte efter at sabotere industristyringssystemer fra Siemens. Det har påvirket alt fra atomanlæg i Iran til it-systemer hos Mærsk.

Hackernes mål med den mystiske orm, som har kostet mange resurser at udvikle, er ikke opklaret, hvilket har fået nogle it-sikkerheds-eksperter til putte den i kategorien cyberkrig fra fjendtlige magter.

Nato oprettede i kølvandet på angrebet mod Estland et center for cyberkrig, som åbnede i Estlands hovedstad i foråret 2008. I Danmark er der - i langt mindre skala - oprettet et såkaldt GovCERT, som er ved at blive løbet i gang.