(https://plus.google.com/115448869619201685712)
(https://plus.google.com/115448869619201685712)

Slik angrep kyberkrigerne Estland

I vår opplevde Estland et massivt digitalt angrep. Rain Ottis sto sentralt i forsvaret:

Fredag 9. november 2007 kl. 15:22
Av Anders Brenna
(mailto:anders.brenna@digi.no)

I vår ble Estland utsatt for det som kanskje kan betegnes som verdens første kyberkrig.

Det var i hvert fall slik Estland opplevde det.

Onsdag denne uken fikk Norge besøk av en av de estiske sikkerhetsekspertene som forsvarte landet sitt under dette angrepet.
Rain Ottis fortalte om erfaringene på årets Paranoia-konferanse, arrangert av sikkerhetsselskapet Watchcom.

Ottis jobber til daglig i en ekspertgruppe for kyberforsvar på **Estonian National Defense College**. Under angrepene jobbet han med å analysere angrepene og de tilhørende hendelsene før, under og etterpå.

Det som utløste kyberangrepet var tilsynelatende et opprør i Tallinn 26. og 27. april, mot at estiske myndigheter ville flytte et krigsmonument – en statue av en russisk soldat – ut av byen.

For russerne, og for mange estlendere av russisk opprinnelse, er denne statuen et viktig symbol for å hedre helter som sloss mot nazistene. Etniske estlendere opplever den derimot som et symbol på 50 år med sovjetisk okkupasjon.

– Hvis det ikke hadde vært en statue der, så hadde det kommet et annet påskudd, sier Ottis.

Opprøret varte bare to dager, men så startet det Ottis og Estland mener var en 22 dager lang kyberkrig.

Les også:

- [30.01.2009] **Kirgisistan rammet av kyberkrig** (/802718/kirgisistan-rammet-av-kyberkrig)
- [13.01.2009] **Spår bølge av politisk nettsabotasje** (/800846/spaar-bolge-av-politisk-nettsabotasje)
- [30.10.2008] **Overvåker alle norske nettsteder** (/792359/overvaaker-alle-norske-nettsteder)
- [12.08.2008] **Georgia anklager Russland for kyberkrig** (/782193/georgia-anklager-russland-for-kyberkrig)
- [13.06.2008] **EU-organ for nettsikkerhet får nytt liv** (/775723/eu-organ-for-nettsikkerhet-faar-nytt-liv)
- [15.05.2008] **Danner global allianse mot kyberterror** (/529016/danner-global-allianse-mot-kyberterror)
- [07.04.2008] **USA øver på offensiv kyberkrig** (/519026/usa-over-paa-offensiv-kyberkrig)
- [14.02.2008] **Hackere styrer tusener av falske DNS-servere** (/509908/hackere-styrer-tusener-av-falske-dns-servere)
- [31.10.2007] **Russiske hackere angriper Ukraina** (/494703/russiske-hackere-angriper-ukraina)
- [28.09.2007] **Estland vil ha FN-konvensjon om IT-krig** (/490368/estland-vil-ha-fn-konvensjon-om-it-krig)
- [17.08.2007] **Norske PC-er ble brukt i angrepet på Estland** (/393058/norske-pc-er-ble-brukt-i-angrepet-paa-estland)
- [16.08.2007] **Drar til Estland for å lære IT-forsvar** (/393018/drar-til-estland-for-aa-laere-it-forsvar)
- [05.07.2007] **Opposisjonen anklager Putin for kyberkrig** (/388354/opposisjonen-anklager-putin-for-kyberkrig)
- [18.05.2007] **Hevder Putin styrer nettangrep** (/382496/hevder-putin-styrer-nettangrep)
- [26.02.2007] **Estland leder an med elektronisk valg** (/370972/estland-leder-

an-med-elektronisk-valg)

Estland er langt fremme i bruk av elektroniske tjenester, og de var derfor veldig sårbare for elektroniske angrep. De har vært helt i tet med blant annet gjennomføring av elektroniske valg.

– Over 98 prosent av estiske banktransaksjoner gjøres elektronisk. Vi leverer selvangivelsen elektronisk og vi har elektroniske pasientjournaler. Vi er helt avhengig av disse elektroniske pasientjournalene, og vi tar i bruk nye hver dag, sier Ottis.

IT-angrep fra hackere med ondsinnede hensikter er ikke noe nytt. Det pågår kontinuerlige angrep mot bedrifter og organisasjoner utført av alt fra såkalte «script kiddies» til organiserte kriminelle.

Estland mener imidlertid at dette var noe helt annet.

– Målene var så variert, at man kan si at hele Estland var angrepet. Det var også indikasjoner om angrepene på forum før angrepene kom, sier Ottis.

Der ble det blant annet oppfordret til å gjøre manuelle angrep, som for eksempel:

«Ping -n 5000 -l 1000 http://www.riik.ee»

– Alle med litt teknisk innsikt ser at den kommandoen ikke ville fungert, men det var nok av teknisk fornuftige metoder også, som for eksempel scriptfiler og lignende, sier Ottis.

Han forteller at det blant annet ble oppfordret til å frivillig la PC-en bli infisert med ondsinnet kode som kunne brukes i kyberangrepet på Estland.

Angrepsmetodene som ble brukt var:

- Defacement – vandalisering av nettsider
- e-post- og kommentarspam
- DoS (Denial of Service) og DDOS (Distributed Denial of Service) – både manuelle og botnetbaserte angrep
- Bruk av exploits og hacking

– Det var mye vanlig «enlarge your penis»-spam, men også innhold spesifikt rettet mot konflikten. Jeg vil ikke kalle det spam når noen sender e-post eller ringer og spør «vet du hvor datteren din er?», sier Ottis.

Isolert sett var ikke angrepene så sofistikerte, men de skapte likevel store problemer for Estland.

– Det var noen exploits som ble brukt, men det var stort sett primitive teknikker. Problemet var at det var omfattende, sier Ottis.

Det var tilsynelatende ingen naturlig sammenheng mellom hvem som ble utsatt for angrepene. Offentlige etater, nettmedier, privatpersoner og småbedrifter ble vilkårlig angrepet. Den eneste fellesnevneren var at domeneadressen sluttet på «.ee».

De mest målrettede angrepene var mot internettleverandørene og bankene. Angriperne gikk mot DNS-servere og sentrale rutere.

– Noen gikk midlertidig ned, men de ble ikke tatt ned permanent. Folk merket ikke det. Det alle merket var bankene, sier Ottis.

Den største banken var nede i halvannen time, mens den nest-største var nede i omtrent en time. Sikkerhetsekspertene klarte å stanse disse angrepene ved å lage begrensede lister over hvilke IP-adresser som fikk lov til å aksessere tjenestene.

– Vi måtte bruke «whitelists», fordi blokkeringslister ikke virket, sier Ottis.

Selv om Estland har klare oppfattninger om hvem som sto bak angrepene, har de ikke 100 prosent håndfaste bevis. Maskinene som ble brukt i angrepene var spredd

rundt om i mange forskjellige land, også Norge. *Se tidligere sak i digi.no:* Norske PC-er ble brukt i angrepet på Estland (/393058/norske-pc-er-ble-brukt-i-angrepet-paa-estland).

Estland var derfor avhengig av internasjonal hjelp, og Ottis bekrefter at Norge, gjennom VDI (Varslingssystem for digital infrastruktur) i NorCERT, var med på å stanse angrepene.

– Jeg er glad for å kunne si at Norge var raske til å reagere, sier Ottis.

Før foredraget, var det flere av deltagerne på sikkerhetsseminaret som hadde spurt om «Hvorfor gikk dere ikke til motangrep?»

Problemet for Estland og sikkerhetsekspertene var at de ikke hadde en synlig fiende de kunne angripe. De hadde – og har – en klar formening om hvem som står bak, men å gå til angrep på det grunnlaget blir helt feil for en rettsstat.

– Det er ikke mulig å få angrepet til å stoppe. Vi må vente til fienden blir lei, sier Ottis.

Etter hvert fikk Estland kontroll på situasjonen og angrepene avtok. 18. mai var kyberkrigen i praksis over. Det gikk bra, blant annet fordi landets sikkerhetseksperter raskt kom i gang med forsvarsarbeidet.

– Estland er et lite land, men fordi vi er små så kjenner alle sikkerhetseksperter hverandre, sier Ottis.

Kyberangrep er billige sammenlignet med konvensjonell krigføring, men det er ikke forsvaret. Dessuten er det et problem at det ikke er noen internasjonale definisjoner for hva som er kyberkrig eller kyberterrorisme.

Estland kan mene så mye de vil om hvem som sto bak det de mener var et angrep, men i denne form for krigføring finnes ikke etablerte krigskonvensjoner.

– Dette skjedde ikke mot oss bare på den tekniske siden. Det er ikke et teknisk problem. Det er et menneskelig problem på politisk nivå, sier Ottis.

Les også:

- [30.01.2009] **Kirgisistan rammet av kyberkrig** (/802718/kirgisistan-rammet-av-kyberkrig)
- [13.01.2009] **Spår bølge av politisk nettsabotasje** (/800846/spaar-bolge-av-politisk-nettsabotasje)
- [30.10.2008] **Overvåker alle norske nettsteder** (/792359/overvaaker-alle-norske-nettsteder)
- [12.08.2008] **Georgia anklager Russland for kyberkrig** (/782193/georgia-anklager-russland-for-kyberkrig)
- [13.06.2008] **EU-organ for nettsikkerhet får nytt liv** (/775723/eu-organ-for-nettsikkerhet-faar-nytt-liv)
- [15.05.2008] **Danner global allianse mot kyberterror** (/529016/danner-global-allianse-mot-kyberterror)
- [07.04.2008] **USA øver på offensiv kyberkrig** (/519026/usa-over-paa-offensiv-kyberkrig)
- [14.02.2008] **Hackere styrer tusener av falske DNS-servere** (/509908/hackere-styrer-tusener-av-falske-dns-servere)
- [31.10.2007] **Russiske hackere angriper Ukraina** (/494703/russiske-hackere-angriper-ukraina)
- [28.09.2007] **Estland vil ha FN-konvensjon om IT-krig** (/490368/estland-vil-ha-fn-konvensjon-om-it-krig)
- [17.08.2007] **Norske PC-er ble brukt i angrepet på Estland** (/393058/norske-pc-er-ble-brukt-i-angrepet-paa-estland)
- [16.08.2007] **Drar til Estland for å lære IT-forsvar** (/393018/drar-til-estland-for-aa-laere-it-forsvar)
- [05.07.2007] **Opposisjonen anklager Putin for kyberkrig** (/388354/opposisjonen-anklager-putin-for-kyberkrig)
- [18.05.2007] **Hevder Putin styrer nettangrep** (/382496/hevder-putin-styrer-nettangrep)
- [26.02.2007] **Estland leder an med elektronisk valg** (/370972/estland-leder-an-med-elektronisk-valg)

Les mer om: kyberkrig (/tag/kyberkrig/)