Kriminalitetsutvikling på nett

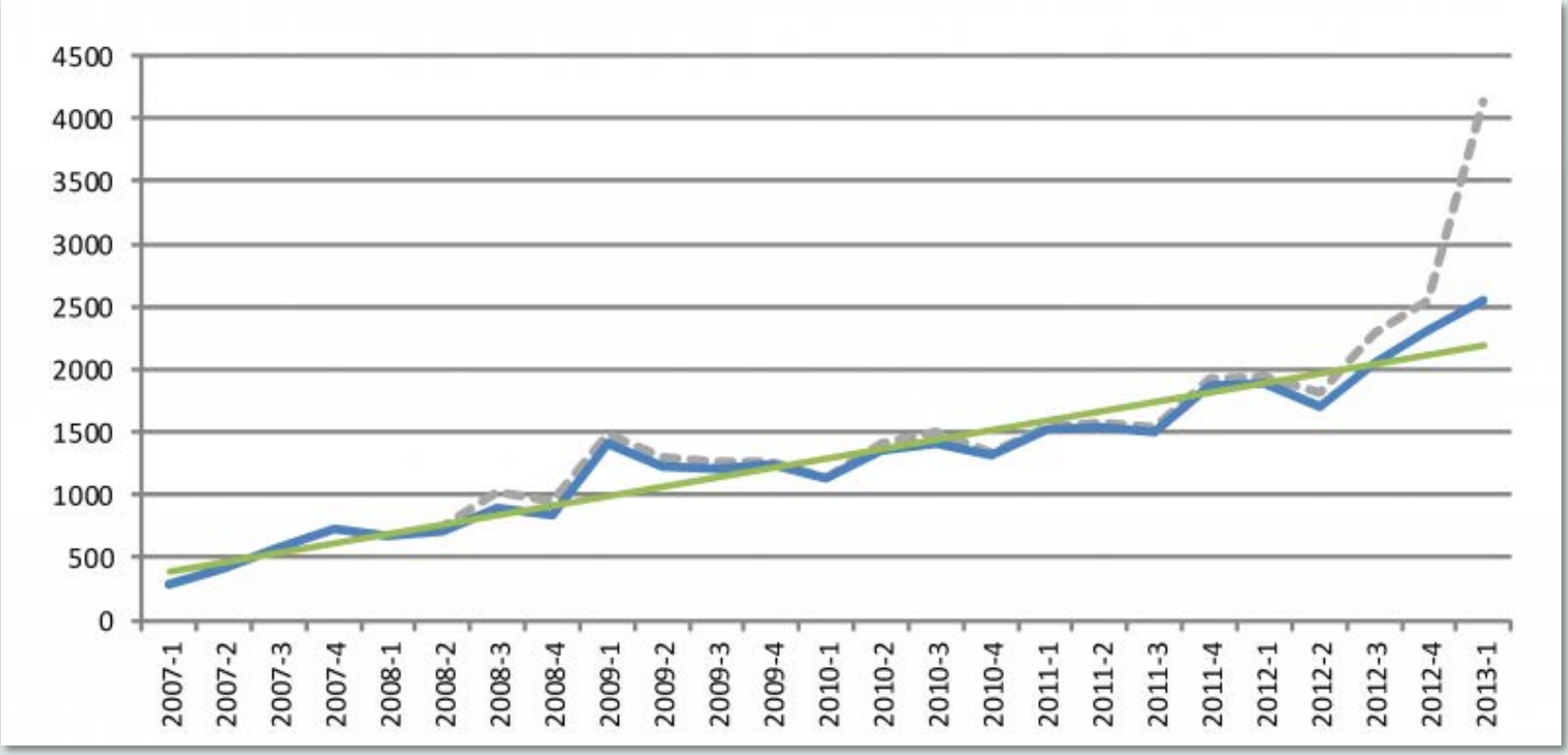
Avdelingsdirektør Eiliv Ofigsbø, NSM/NorCERT

Hvem er vi?

- *NorCERT er en del av Nasjonal sikkerhetsmyndighet (NSM) og er Norges nasjonale senter for å håndtere alvorlige dataangrep mot samfunnskritisk infrastruktur og informasjon.*
- *...NorCERT skal produsere et oppdatert nasjonalt IKT-trusselbilde.*
- *...Det skal etableres en koordineringsgruppe med representanter fra Etterretningstjenesten og Politiets sikkerhetstjeneste som skal sikre en helhetlig beskrivelse av IKT-trusselbildet.*

- *En del av Operativ avdeling I NSM*
- *Inkluderer Varslingssystem for Digital infrastruktur*

Saker under operativ håndtering



Grafen viser saker under operativ håndtering. På grunn av den markante økningen i saker knyttet til kompromitterte norske websider som enten sprer skadevare eller på annet måte misbrukes av kriminelle, er disse tallene skilt ut. Den heltrukne blå linja viser saker som ikke kan knyttes til kompromitterte websider. Den striplete grå linja er det totale antall saker.

Hva er truslene?

Krigføring

Info OPS

Sabotasje

Spionasje

Finansiell kriminalitet

Politiske protester

Rampestreker

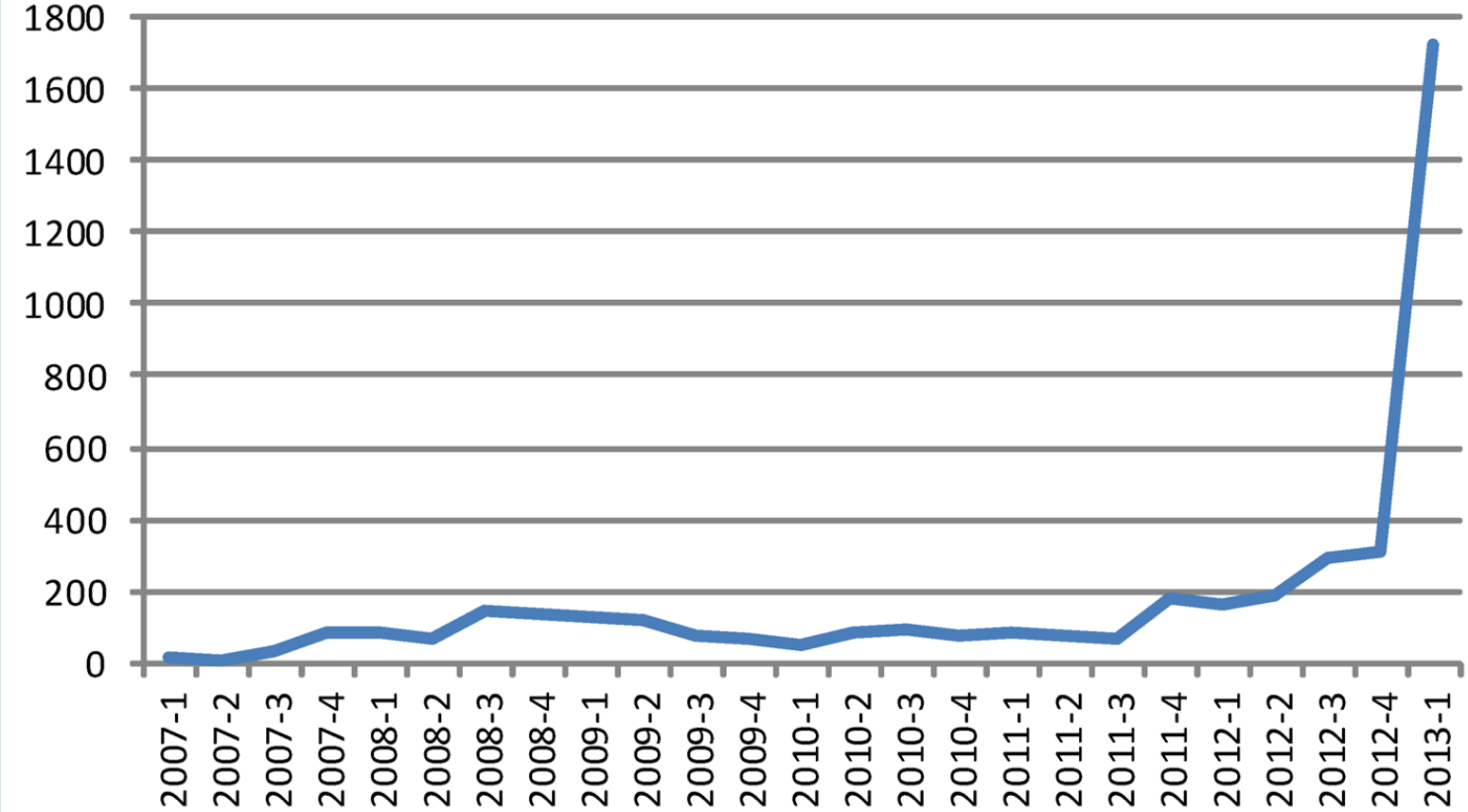
Trusler mot finansiell infrastruktur

- Kredittkortsvindel
- Nettbankkunder
- Bedriftskunder
- Banksystem

- Målrettede angrep

Skadevare – Økning i spredning fra norske nettsteder

- **En kraftig økning i antall rapporter om infiserte nettsider i 2013**



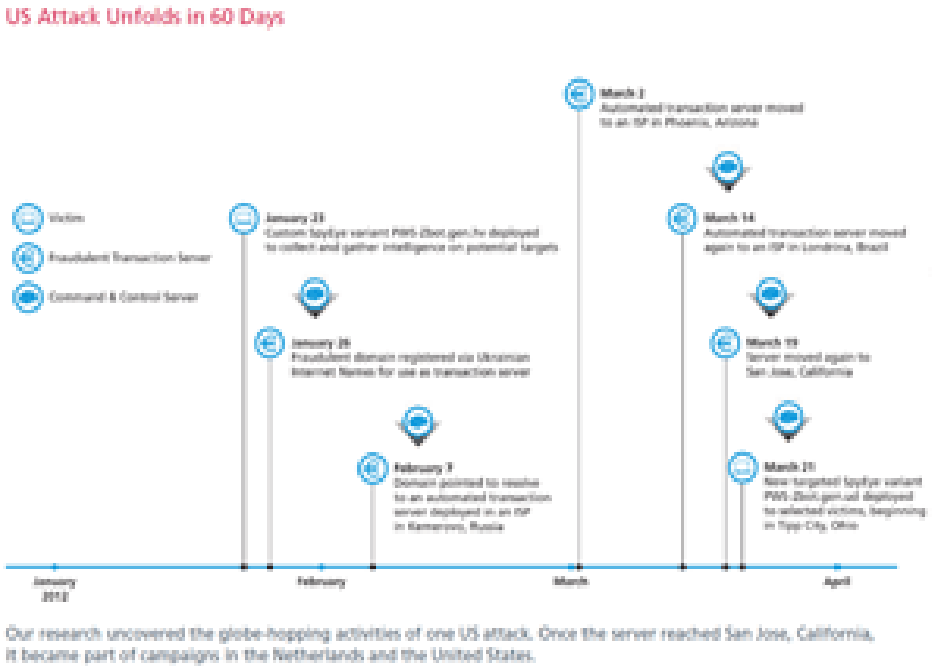
Trusler – økonomisk kriminalitet

Trusler – økonomisk kriminalitet

Operation High Roller Uncovers New Server-Side Fraud Attacks

This report, "Dissecting Operation High Roller," was jointly released by Guardian Analytics and McAfee. It describes a sophisticated international fraud scheme that uses cloud-based, automated attacks to target high-balance accounts, hence the "high roller" title.

This is a serious new threat that is actively targeting American financial institutions. To the best of our knowledge the scheme has already netted nearly $80M worldwide, and it could be much higher. The innovative, sophisticated nature of this scheme further escalates the importance of implementing layered security, including anomaly detection solutions that have been proven to be able to detect these attacks.



Our research uncovered the globe-hopping activities of one US attack. Once the server reached San Jose, California, it became part of campaigns in the Netherlands and the United States.

Trusler – økonomisk kriminalitet

ComputerSweden

Jörgen Lindqvist:
Äntligen får Telia r
konkurrens

CS JOBB | CS LIFE | CS PODCAST | TEKNIK | OPINION | EVENT | ANNONSERA | MER FRÅN CS

Publicerad 2013-05-16 03:00

Nordeakunders konton i hackares händer

Av Jonas Ryberg

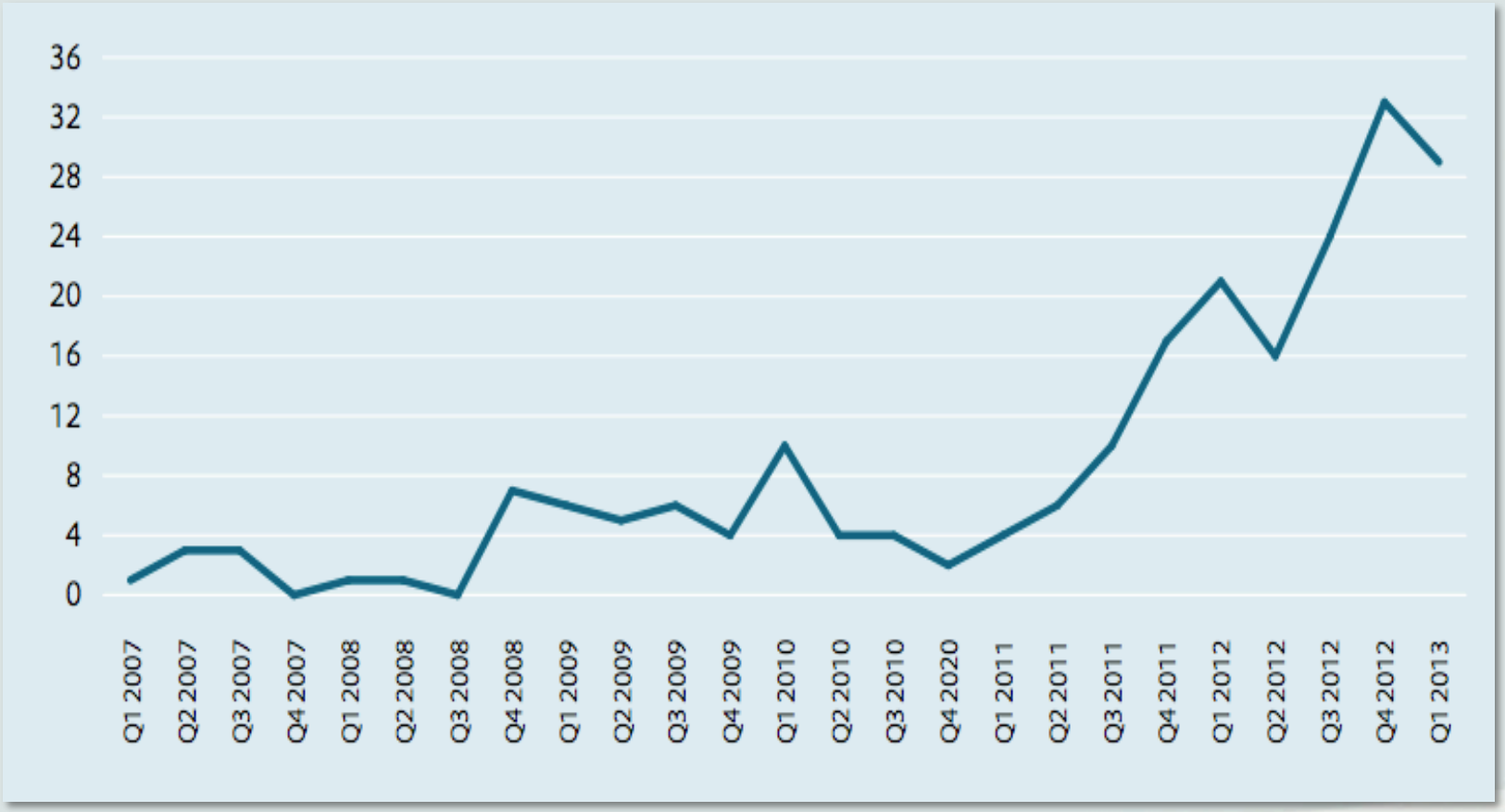
NYHETER **Under flera månader förra sommaren hade hackare tillgång till Nordeas system för betalningar och till kundernas konton. Det påstår utredarna i den förundersökning som ligger till grund för åtalet mot Pirate Bay-grundaren Gottfrid Svartholm Warg.**

ANNONS

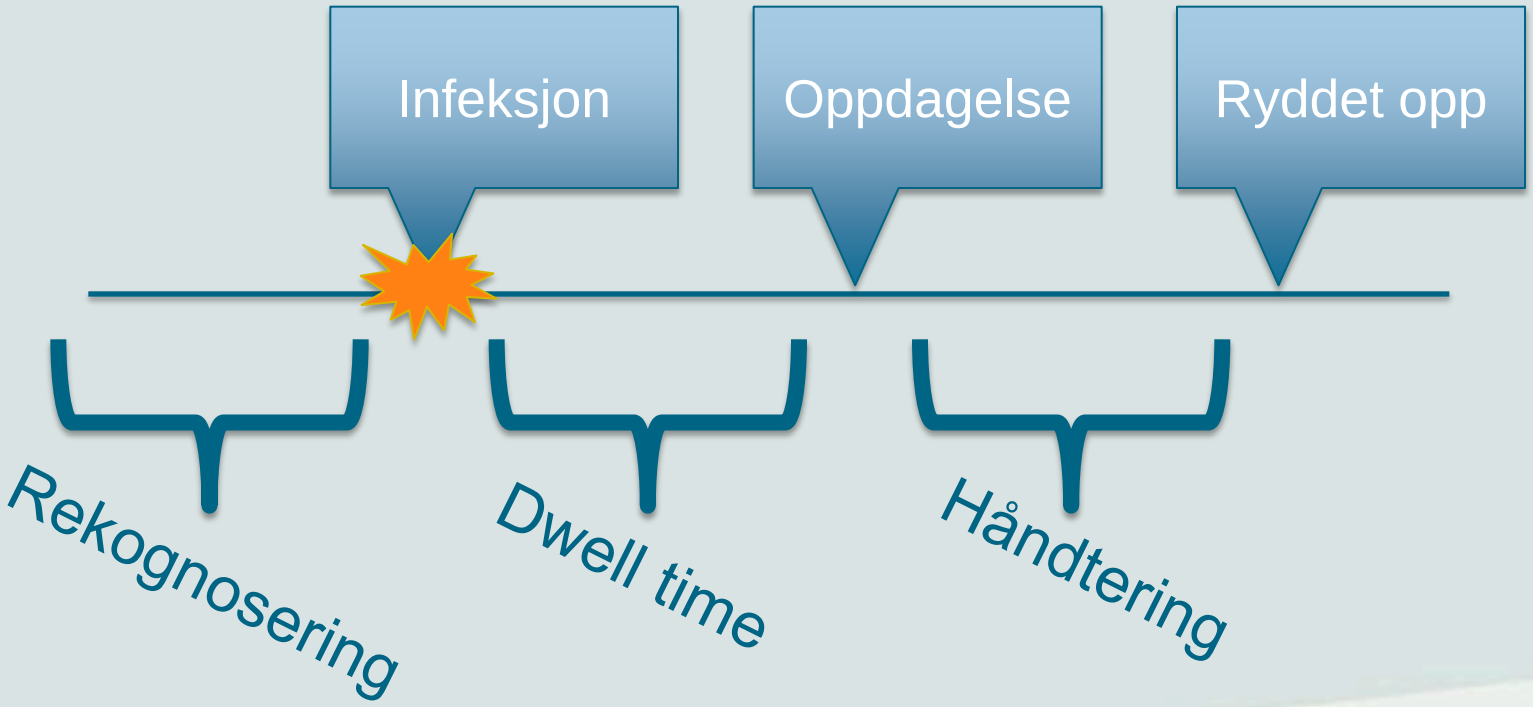
Nettaktivisme / DDOS

- Mye medieomtale rundt angrep mot svenske myndigheter
- Tilsvar etter at politiet raidet hosting leverandøren PRQ og tok ned flere fildelingstjenester
- Mer irriterende enn alvorlig

Antall håndterte alvorlige hendelser



Digital spionasje - Hendelsesforløp



Eksempler fra virkeligheten

Hendelse #1:

- Virksomhet kompromittert noen dager
- Eksternt firma varslet NorCERT om hendelsen

Hendelse #2:

- Virksomhet kompromittert i fem måneder
- Hendelse oppdaget i NorCERTs sensorsystem (VDI)

Hendelse #3:

- Virksomhet kompromittert i 18 måneder
- Ekstern samarbeidspartner varslet NorCERT

Hendelse #4:

- Virksomhet kompromittert i 15 måneder
- Hendelse oppdaget av egne ansatte

Hendelse #5:

- Virksomhet kompromittert i over en måned
- NorCERT analysert liknende skadevare og ba virksomhet sjekke egne systemer

Digital spionasje

norman

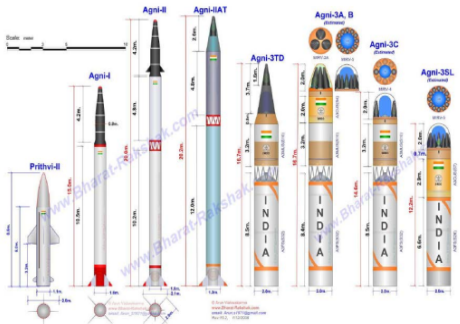
May 2013

OPERATION HANGOVER

Unveiling an Indian Cyberattack Infrastructure

Snorre Fagerland, Morten Kråkvik, and Jonathan Camp
Norman Shark AS

Ned Moran
Shadowserver Foundation



Part of a PDF decoy from one of the malicious installers (md5 06e80767048f3edefc2dea301924346c).

Svært mange angrep på amerikanske interesser skal stamme fra nabolaget til denne blokka, der en enhet fra den kinesiske hæren holder til. Foto: CARLOS BARRIA

Amerikansk rapport: Fra denne blokken kommer angrepene

Kilde: Dagensit.no

Hva kan vi gjøre?

Foto: www.colourbox.com

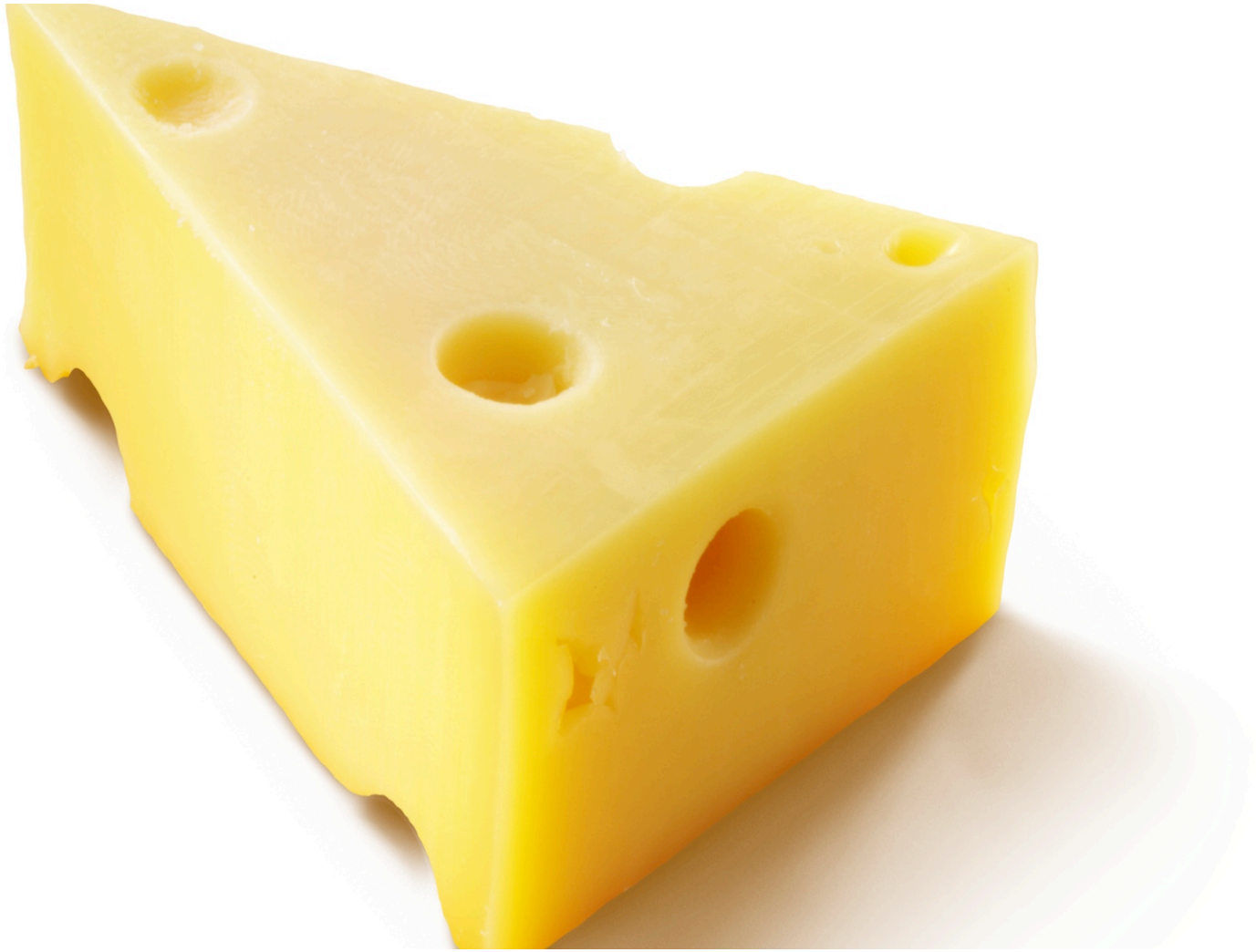


Foto: www.colourbox.com

Hvordan sikre seg?

- Lederforankring
- Verdivurdering
- Separering av operasjonelt nettverk fra administrativt nett/Internett
- IDS/IPS
- Oppdatert programvare
- Oppdatert anti-virus og brannmuroppsett
- Rutiner for rapportering av sikkerhetshendelser
- Rutiner for hendelseshåndtering
- Øvelser
- Penetrasjonstesting
- Opplæring
- **Sikkerhetsbevisste og årvåkne sluttbrukere!**

18