Målrettede angrep

CIO forum 6.mars 2013

Tore Terjesen
Head of MSS & SOCs - Nordics
tore.terjesen@secode.com

SECODE
An Integralis Group Company

Secode – the pure play security company

- **En ledende og relevant MSSP i Norden**
  - Malware research team
  - Threat intelligence team

- Sikkerhetspartner, ikke leverandør
- 1/3 av alla organisationer på Stockholms och Oslobörsen som kunder

- Mer enn 27 år på vakt – siden 1986
- 100+ dedikerte sikkerhetsspesialister

- 1 redundant 24x7 SOC

- Alle ansatte hos Secode har gyldig sikkerhetsklarering t.o.m ”HEMMELIG”

- Secode en del av NTT og Integralis

Agenda

- Threat intelligence
- Trusselbildet
- Forskjellige typer målrettede angrep

Målrettede angrep??

- Risikoreduserende tiltak må tilpasses etter virksomhetens:
  - Verdier
  - Sårbarheter
  - Trusler

Threat Intelligence

trusler

$$$

verdier

virkemidler

metoder

skadevare

sårbarheter

Målrettede angrep i Norge er en realitet

- I 2012 håndte
så mange alvo
typisk relatert
2012 som i 201
saker av denne
Marte Meo i NS

FOTO: ROBERT M

Her går hacker-alarmen oftere enn før

Olje og gass. Kraftverk. Forsvarets våpensystemer. Antall hackerangrep mot viktige samfunnsvirksomheter er doblet.

Trusselbildet

”Enkelte stater støtter næringslivet sitt gjennom statlig etterretningsvirksomhet.

En slik virksomhet kan få betydelige følger for norske selskapers og bedrifters konkurranseevne.”

Kilde: http://www.pst.no/trusler/spionasje/

Trusselbildet

”Angrepene har vært rettet spesielt mot olje og gass-sektoren, energi-sektoren og forsvarsindustrien. Angrepene har ved flere tilfeller skjedd i forbindelse med at firmaene utfører større kontraktsforhandlinger. Skreddersydde e-poster med virus er sendt til utvalgte personer i store norske bedrifter for å stjele all informasjon på datamaskinene. Det dreier seg eksempelvis om dokumenter, industritegninger og brukernavn og passord.”

Kilde: https://www.nsm.stat.no/Aktuelt/Nytt-fra-NSM/Samme-aktor-bak-flere-datainnbrudd/

Trusselbildet

Dwell time:

“APT1 maintained access to victim networks for an average of 356 days. The longest time period APT1 maintained access to a victim’s network was 1,764 days, or four years and ten months.”

Kilde: Mandiant

Målrettede angrep

- Vannhullssangrep
- Spear fishing
- Informasjonsuthenting via Web – SQL Injection
- Lukkede/sikre nett
- Social Engineering

Vannhullsangrep??

Vannhullsangrep

Vannhullsangrep

Mange ble hacket

Som følge av slett datasikkerheten i Nobel- komiteen, kan over 300 personer og selskaper ha blitt utsatt for dataspionasje.

Lone Kira Wik (Foto)
Publisert: 14.nov. 2010 00:44 **Oppdatert:** 12.okt. 2011 20:30

De 300 privatpersonene, bedriftene og organisasjonene kan ha blitt utsatt for dataspionasje fordi de besøkte datasidene til Nobelkomiteen og Nobelinstituttet 26. og 27. oktober. Da fikk de nemlig installert en spionprogramvare, som ga utenforstående full tilgang til deres datamaskiner.

Spionasjen på Nobelinstituttet har pågått i mye lengre tid og er mye mer omfattende enn tidligere kjent. Ifølge Nasjonal sikkerhetsmyndighet gikk det elleve dager fra nettsidene ble hacket, og til man oppdaget det svært avanserte innbruddet.

– Fra mandag ettermiddag til tirsdag morgen kan jeg anslå at vi kan ha hatt opp mot 300 besøkende med Firefox-versjon 3.5. og 3.16, sier bibliotekar og IT-ansvarlig Bjørn H. Vangen ved Nobelinstituttet.

– Vi har ingen mulighet til å spore hvem de er. Det som er mest beklagelig med saken, er at folk som har besøkt våre nettsider kan ha blitt skadelidende.

Spear fishing

Spear fishing

Løsninger sett fra brukerens ståsted:

- Vær varsom med å åpne vedlegg
- Ingen antivirusdeteksjon..
- Send e-posten til sikkerhetsansvarlig for analyse

Spear fishing

Løsninger sett fra CIO/CISO/IT:

- Opplæring av ansatte (fokusgrupper?)
- Hold datamaskiner oppdatert (fokusgrupper?)

Spear fishing

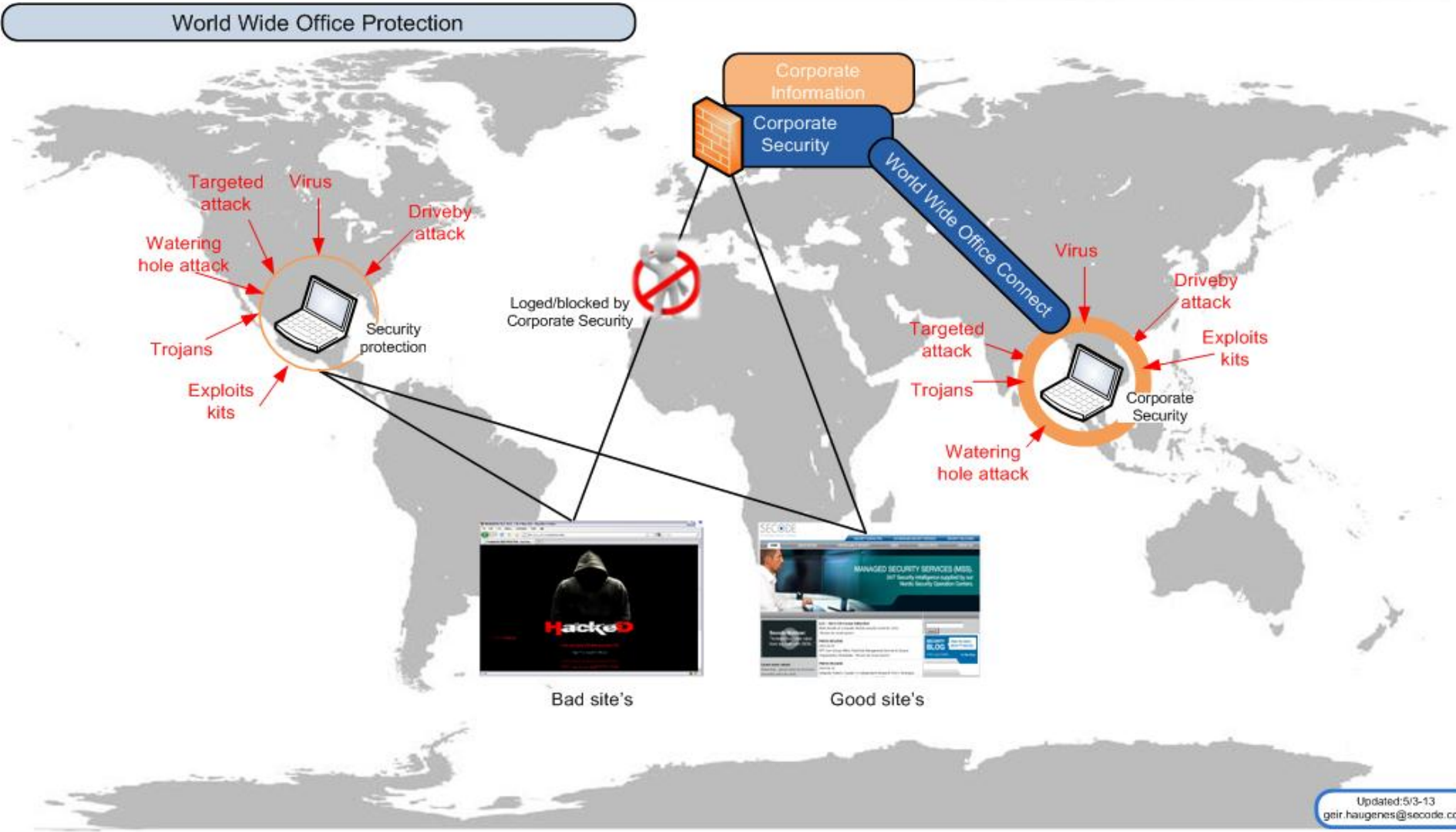
Løsninger sett fra CIO/CISO/IT:

- Logg mest mulig!
  - Spesielt FW og proxylogger
  - Sett loggene i et større perspektiv sammen med IDS/IPS logger, Antiviruslogger, AD logger..
  - Ny triggerinformasjon kan brukes til å søke i gamle data

Målrettede angrep og zero days kan oppdages!

- Alle vellykkede angrep resulterer i nedlasting av skadevare
- Automatisk oppførselsanalyse av filer virtuelle miljøer og sandkasser
- Følges opp av analytiker
- Kombineres med proxy, FW, IDS/IPS logger med mere..

Full kontroll??



SECODE
An Integralis Group Company

SQL Injection

SQL Injection

- Utnytter svakhet/feil i webapplikasjoner for å få tilgang til databasen bak
- #1 angrepsmetode for å stjele (kunde)data siden 2005
- Anvendt i 83% av alle vellykkede angrep hvor kundedata har havnet på avveie..

Open Web Application Security Project - OWASP

- A 1 - Injection Flaws - particularly SQL
- A 2 - Cross Site Scripting (XSS)
- A 3 - Broken Authentication and Session Management
- A 4 - Insecure Direct Object Reference
- A 5 - Cross Site Request Forgery (CSRF)
- A 6 - Security misconfiguration
- A 7 - Insecure Cryptographic Storage
- A 8 - Failure to Restrict URL Access
- A 9 - Insufficient Transport Layer Protection
- A10 - Unvalidated Redirects and Forwards

SQL injection

Løsninger:

- Skriv gode kravspesifikasjoner
  - Inkluderer krav til sikkerhet!
- Utfør applikasjonstester
  - Også ved endringer/oppdateringer…

Paradoks..

Når sikkerhet ikke er tilpasset forretningsprosessene..

For streng sikkerhetspolicy fremkaller “nødløsninger” som øker risikoen dramatisk

Lukkede eller svært sikre nett

Afghanistan-styrkene hacket

De norske styrkene i Afghanistan er forsøkt kartlagt av fremmed etterretning. Her vokter norske styrker utenriksminister Støre i Nord-Afghanistan i 2009.

Foto: Junge, Heiko/NTB scanpix

Lukkede eller svært sikre nett

- Lukkede nett har erfaringsmessig dårlig/lavt patchenivå
- Det er fritt frem når inntrengeren først er innenfor
- Bruken av lukkede nett endres ofte over tid
    - Det oppstår behov for å flytte data
    - Arkitekturen rundt endrer seg
- Det gjennomføres ikke risikoanalyser ved endringene…
- Dette ser vi medfører nødløsninger som åpner opp for angrepsvektorer som ellers kunne vært unngått

Ikke glem ”Social Engineering”

Zero-day exploits get all the sexy headlines, but social engineering gets most of the results:)

Sosial manipulasjon + teknologi + kompetanse = resultater

Social Engineering – resultater

- Fått tilgang til firmabil
- Fått nøkkelen til hvelv
- Hatt fri adgang til personalmapper
- Blitt så godt kjent at vaktselskapet ga oss nøkler til bygget
- Høstet brukernavn og passord fra 100% av de ansatte som ble testet
- Blitt ringt tilbake i kjølvannet av webmailtester
- Fått tilgang til servere, printere, kablingsrom og klientmaskiner
- Gjennomført DNS-endringer
- Fått tilgang til personsensitive dokumenter markert ”Unntatt offentligheten”
- Blitt ansatt!
- Og mye mer….

Oppsummering

- Målrettede angrep er en realitet
- Skaff deg oversikt over truslene
- Prioriter risikoreduserende tiltak vs. forbud (som omgås)
- Logg relevante data, og sørg for at de anvendes, ikke bare lagres..
- Tving all datatrafikk gjennom bedriftens nettverk
- Ikke glem den menneskelig faktoren i all teknologien ☺

Questions

Discussion

Next steps

SECODE
An Integralis Group Company