ØKOKRIM

Den sentrale enhet for etterforsking og påtale av økonomisk kriminalitet og miljøkriminalitet

www.okokrim.no

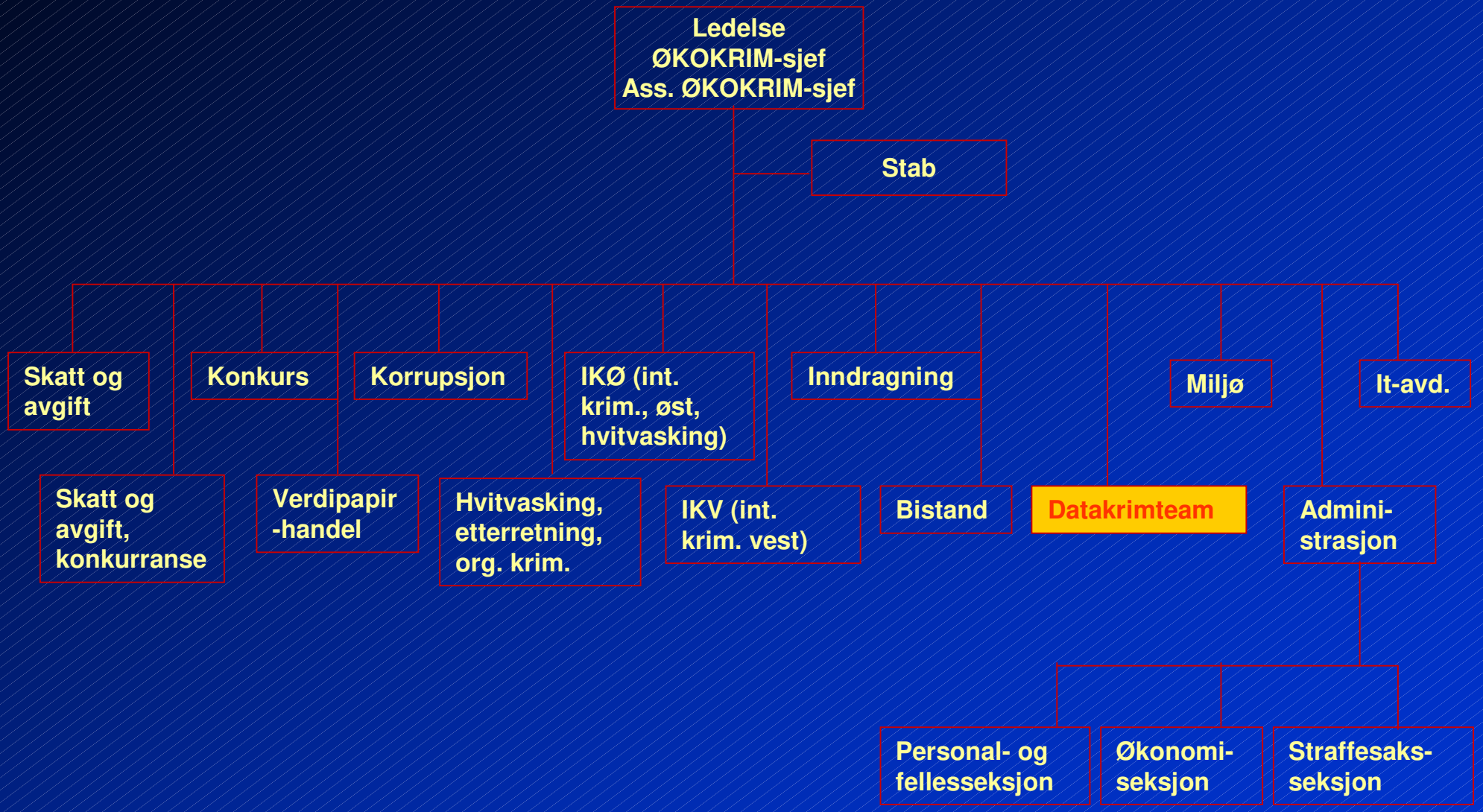
Datainnbrudd:

Gjerningsmenn, lovbestemmelser og bevissikring

Svein Yngvar Willassen

spesialetterforsker

ØKOKRIM


Ledelse
ØKOKRIM-sjef
Ass. ØKOKRIM-sjef
Stab
Skatt og avgift
Konkurs
Korrupsjon
IKØ (int. krim., øst, hvitvasking)
Inndragning
Miljø
It-avd.
Skatt og avgift, konkurranse
Verdipapir -handel
Hvitvasking, etterretning, org. krim.
IKV (int. krim. vest)
Bistand
Datakrimteam
Admini-strasjon
Personal- og fellesseksjon
Økonomi-seksjon
Straffesaks-seksjon

Datakrimteamet, ØKOKRIM

Tverrfaglig sammensatt

- 2 jurister (statsadvokat + politiadvokat)
- 4 etterforskere med datafaglig bakgrunn
- 3 etterforskere med politifaglig bakgrunn
- 1 konsulent

Arbeidsoppgaver

- **Teknisk bistand til Økokrim og politiet**
  - ransaking og beslag i datamiljø
  - sikring av datalagringsmedier (speilkopiering)
  - analyse av databeslag, dvs finne bevisene
- **Etterforskning av egne straffesaker**
- **Påtale (aktorering av egne saker)**
- Kompetansehevende tiltak, bl.a. v/PHS
- Rådgivning / foredrag / forebyggende virksomhet

En vakker dag...

ØKOKRIM

Hvem har vi med å gjøre ?

Hvem gjør datainnbrudd?

TRE TYPER :

- "The Script-kiddie"

- "The insider"

- "The profesional"

Script Kiddie

En person som har skaffet seg kjennskap til noen verktøy som kan brukes til datainnbrudd. Skanner hele internett etter denne typen svakheter, og bryter seg inn på maskiner han kommer over.

- Ofte ungdom
- Har ofte tilgang på stort antall maskiner
- Gjør uforvarende stor skade
- Kjører DoS angrep mot andre script kiddies

Innsideren

En ansatt eller tidligere ansatt i et firma som har unik kjennskap til datasystemer/rutiner kan utføre forandringer som ikke oppdages av andre

- Som regel vinnings- eller hevnmotiv
- Benytter kjennskap til system til å gjøre datainnbrudd / uautorisert endring
- Kan være vanskelig å oppdage

Den profesjonelle

Angriper systematisk et bestemt mål ved å over tid kartlegge svakheter, og deretter angripe svakeste punkt

- Fjerner sine spor, benytter flere mellomledd

- Utfører ikke skadeverk, stjeler bare informasjon

- Ressursbruken ved denne typen virksomhet gjør det vanskelig/umulig å gjøre dette alene. Det er derfor snakk om organisert virksomhet.

Datasikkerhet

Beskyttelse mot tre ulike "gjerningsperson profiler".

Script Kiddie

Effektiv beskyttelse mot script-kiddies forutsetter en av to følgende strategier:

- Nøye oppfølgning av alle kjente sikkerhetsfeil i alle system man administrerer.

- Brannmur som kun tillater eksplititt godkjent trafikk å passere. Mest effektiv kombinert med intrusion detection. Oppfølgning av sikkerhetsfeil er fortsatt nødvendig, men ikke like stort omfang.

Innsideren

De samme tiltak som mot script-kiddies pluss:

- Streng administrasjon av ansattes rettigheter.

- Gradering av følsom informasjon. Loggføring av ansattes behandling av følsom informasjon.

- Når noen slutter: Alle rettigheter fjernes umiddelbart. Kjente passord skiftes. Vurdere å endre rutiner på følsomme områder.

Den profesjonelle

Som for script-kiddies og innsidere, pluss:

- Trusselvurdering. Hvilke områder er utsatt, og hvem kan tenkes å angripe dem?

- Analyse av loggdata for å oppdage uregelmessigheter, og takle disse.

- Mottiltak: Etablere apparat for å ta imot tips/rapporter om virksomhet. Selv drive kontra-etterretning. (På lovlig vis.)

Trusselvurdering

Hvem er farligst?

Skade – ødelagt utstyr/data

Script kiddie: Mangler kontroll, prøver å slette spor.

Innsider: Kan slette data ut fra hevnmotiv

Proffen: Unngår skadeverk for å unngå å bli oppdaget

Skade – uautorisert endring

Script kiddie: Skjønner sjelden nok av systemet til å utføre fornuftige endringer

Innsider: Kan utføre endringer på datasystem i vinnings hensikt

Proffen: Kan utføre endringer for å nå sine mål / utføre ordre

Informasjon på avveie

Script kiddie: Skjønner sjelden nok av systemet til å forstå hvilken verdi informasjon har

Innsider: Kan selge/spre informasjon til utenforstående i vinnings hensikt

Proffen: Kan få tak i informasjon og bruke den til egne formål

Hvor mange er de?

Script kiddie: Potensielt alle gutter i alderen 13-22. Erfaringsmessig har ca 50% av alle på denne alderen som tilbringer mer enn 2 timer hver dag på Internett forsøkt å komme inn på andre maskiner.

Innsider: Potensielt i alle bedrifter. Erfaringsmessig finner man dem oftest blant de datakyndige, og særlig i aldersgruppen 20-35 år. Typetilfellet er dem som kommer på kant med overordnete.

Proffen: Finnes i militære etterretningsorganisasjoner. Muligens også i større kriminelle nettverk.

Lovbestemmelser

Straffelovens §145

...ved bryte en beskyttelse eller på lignende måte skaffer seg adgang til data eller programutrustning som er lagret eller som overføres ved elektroniske eller andre tekniske midler...

- Rammer uatorisert tilgang til datasystemer, forutsatt at systemet er beskyttet.
- Bruk av exploits for å komme seg inn på system
- Bruk av passord for å logge seg på urettmessig
- Avlytting av datanettverk
- Str. ramme: 6 mnd. Ved skade eller vinning: 2 år

Straffelovens §145, §49

Forsøk på datainnbrudd rammes.

- Bruk av exploit mot system, uansett om det lykkes
- Forsøke forskjellige passord for innlogging
- Bruk av skannere som innebygget kjører exploits
- Portscanning rammes ikke, jfr Norman-dommen

- VIKTIG: **forsett**

Straffelovens §261, §393

Den som rettsstridig bruker eller forføyer over en løsøregjenstand som tilhører en annen...

- Rammer uvedkommendes bruk av datasystem
- Rammer innsideres bruk av datasystem i strid med gjeldende regler.

- Str. ramme: bøter (§393), Ved betydelig skade eller vinning: 3 år (§261)

Straffelovens §291, §292

For skadeverk straffes den som rettsstridig ødelegger, skader, gjør ubrukelig eller forspiller en gjenstand som helt eller delvis tilhører en annen.

- Rammer autorisert endring/sletting i datasystem
- Rammer DoS – angrep (..*gjør ubrukelig*..)

- Str. ramme: 1 år (§291), Grovt skadeverk: 6 år (§292)

Straffelovens §270, §271

For bedrageri straffes den som i hensikt å skaffe seg eller andre en uberettiget vinning ... ved bruk av uriktig eller ufullstendig opplysning, ved endring i data eller programutrustning eller på annen måte rettsstridig påvirker resultatet av en automatisk databehandling, og derved volder tap eller fare for tap for noen.

- Rammer autorisert endring/sletting i datasystem i vinnings hensikt.
- Typisk eks: endring i bank-programvare.
- Str. ramme: 3 år (§270), Grovt bedrageri: 6 år (§271), Grovt uaktsomt bedrageri: 2 år (§271a)

Sikring av bevis

Hvordan sikre bevis ved datainnbrudd?

1. Ikke gjør noe

Ikke få panikk, du har alltids tid å tenke deg om. Tenk taktikk! Ikke la forbryteren få sjansen til å slippe unna.

Hvis maskinen fortsatt er oppe:

- Ikke dra ut pluggen

Hvis systemet er skadet / slettet:

- Ikke reinnstaller systemet

Kontakt politiet !!

2. Status

Før en kompromittert maskin tas ned bør en sikre informasjon som forsvinner når maskinen skrus av. Momenter: *w, netstat, ps, ifconfig*

Disse kommandoene bør ideelt sett kjøres statisk lenket fra et separat medium, og utskriften ikke lagres til maskinens harddisk. Man kan evt. fotografere skjermen.

3. Vurdere ”felle”

I mange tilfeller bør det vurderes å la den kompromitterte maskinen stå, og iverkssette logging av all trafikk inn og ut av maskinen.

Dette er særlig aktuelt for maskiner som har vært besøkt av uvedkommende, som muligens kan komme igjen.

4. Speilkopiering

Politiet benytter et verktøy som kopierer alt innhold på en harddisk, bit for bit, til å sikre bevis. Maskinen kan deretter reinnstalleres.

Har man ikke et slikt verktøy er det bedre å reinnstallere systemet på et annet medium.

5. Anmeldelse

For at politiet skal etterforske og påtale straffbare forhold trengs det en anmeldelse med påtalebegjæring. Dette må oversendes skriftlig, eller ved fremmøte.

For selskaper er det styret som har påtalefullmakt. Hvis andre skal begjære påtale må det foreligge fullmakt fra styret.

6. Etterforskning

- Analyse av angrepet maskin
- Sporing
- Vitneavhør
- Pågripelse, Ransaking
- Avhør
- Vitneavhør
- Analyse av beslag (datamaskiner, annet)

7. Påtale

- Påtaleavgjørelse: henleggelse, forelegg, tiltale
- Hovedforhandling i tingrett
- Ankeforhandling i lagmannsrett
- Kjæremål til Høyesterett

- Fullbyrdelse av straff