

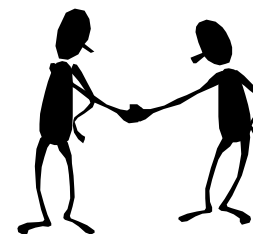
Senter for informasjonssikring

Om IKT-trusler og mørketall innen datakrim

Maria Bartnes Dahl
maria.b.dahl@sintef.no

SIS: Bakgrunn

- Etablert i 2002
 - Avtale mellom NHD og SINTEF
 - Samarbeid med UNINETT
- Evaluering i løpet av 2004
- Foreløpig ingen avklaring for 2005
 - Hvem – hva – hvor?



SIS: Hovedoppgaver

- Fremskaffe et helhetlig bilde av trusler som berører IKT-systemer i Norge.
 - Formidle informasjon, kompetanse og kunnskap om trusler og mottiltak.
 - Ha kontakt og samarbeid med tilsvarende organisasjoner i andre land.
- SIS skal stimulere til sikkerhetskultur.

Produkter fra SIS



- Trusselrapporter
 - inkl. månedlige oppsummeringer
- Nyheter/pressestoff
- Veiledninger
- Korte artikler om aktuelle temaer
- Diskusjonspartner
- Foredrag på konferanser/seminarer/kurs
- Lenker til andre nyttige nettsider
- Kontaktnett nasjonalt og internasjonalt
- Samarbeid med FoU-institusjoner



Senter for informasjonssikring (SIS)

har ansvar for å koordinere aktiviteter knyttet til IKT-sikkerhet i Norge og arbeider med å kartlegge det totale trusselbildet mot IKT-systemer i det norske samfunnet.

[les mer](#)

[rapportere hendelse](#)

[bransjesøk](#)

[ordliste](#)

[kontaktadresser](#)

[e-postvarsling](#)

[sidekart](#)

[siste trusselrapport](#)

søk

i hele norsis.no ▼

nyheter

22.11.04

Orm kompromitterer reklameleverandører og nettsteder

Nett-avisen The Register og andre nettsteder kom på mandag i skade for å utsette sine lesere for ondartet kode som utnytter en kjent sårbarhet i Internet Explorer

[les mer](#)

15.11.04

Ny "stealthy" phishing-taktikk

09.11.04

Nye versjoner av MyDoom utnytter sårbarhet i IE

[nyhetsarkiv](#)

sårbarheter

24.11.04

Bufferoverflyt i Winamp

Det er avdekket en sårbarhet i Winamp som kan gi angripere utenfra tilgang til en maskin. Sårbarheten ligger i muligheten for bufferoverflyt. [les mer](#)

23.11.04

Alvorlig sårbarhet i Java Plug-in

18.11.04

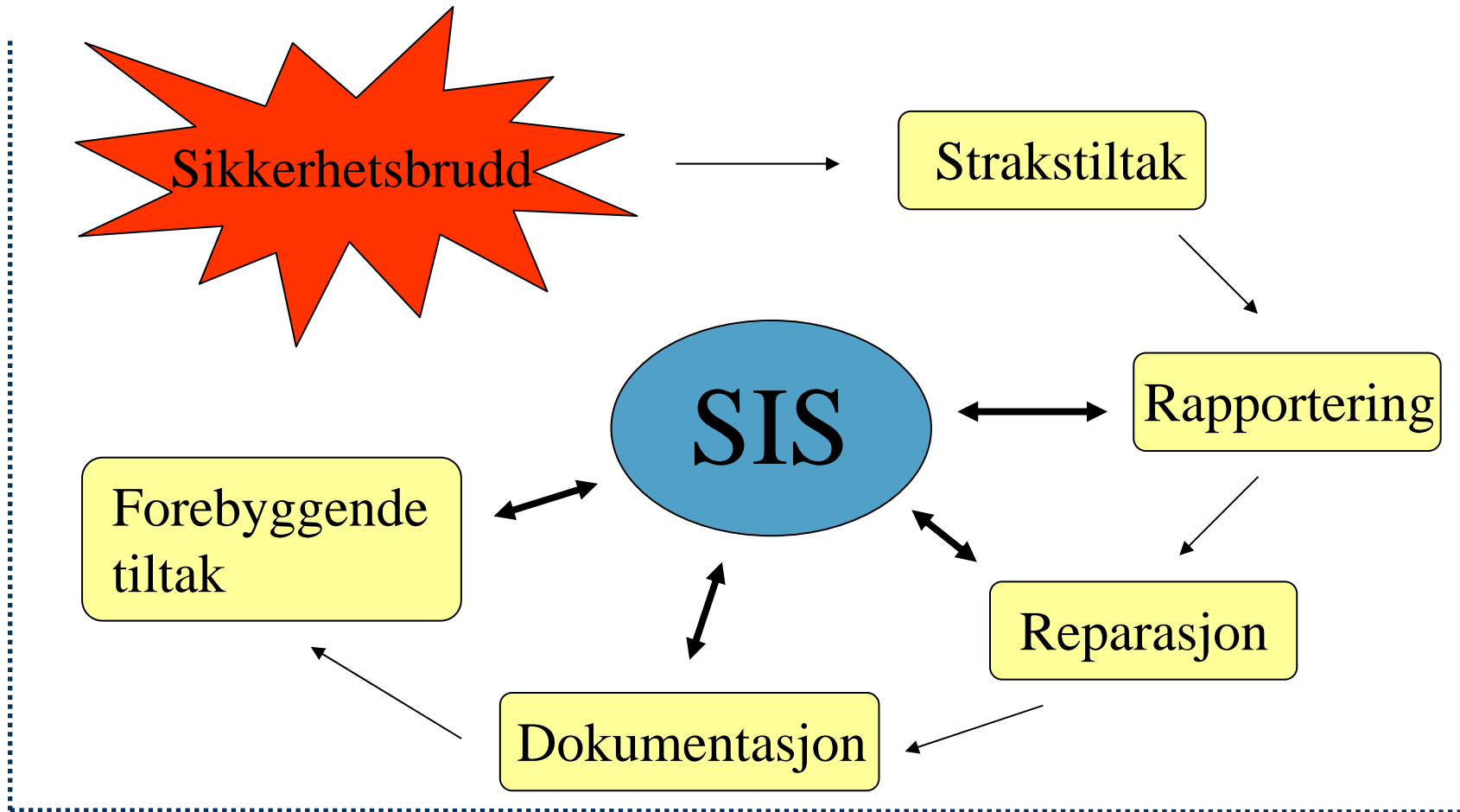
Flere sårbarheter i Internet Explorer

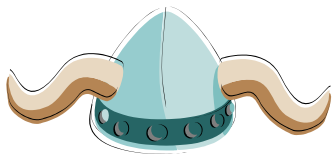
[arkiv](#)

Hendelsesrapporter

- SIS trenger informasjon om sikkerhetsrelaterte hendelser i Norge
 - Konfidensialitet
 - Integritet
 - Tilgjengelighet
- Analysere hendelser og mottiltak:
- Gi tilbakemelding til de som rapporterer
- Ingen vidererapportering til andre instanser
- Anonymisering av data

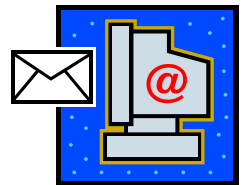
Hvor kommer SIS inn?





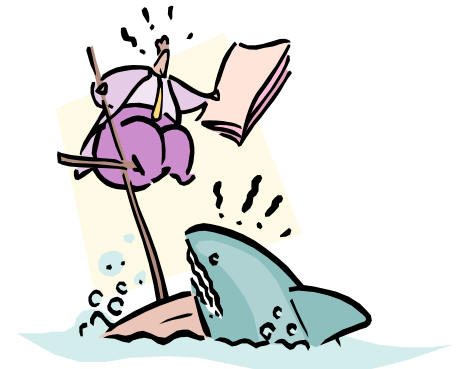
Spesielle forhold i Norge

- Tar svært raskt i bruk ny teknologi
 - Norske, svenske og danske tar raskest i bruk et nytt produkt etter at det er introdusert (University of Southern California, Erasmus University Rotterdam og Cambridge University, www.digi.no)
- Høy utbredelse av bredbånd
 - Forventet utbredelse 45 % innen 2008 (Forrester Research, www.handel.no)
- Internett-baserte verktøy en viktig del av hverdagen for norske arbeidstagere



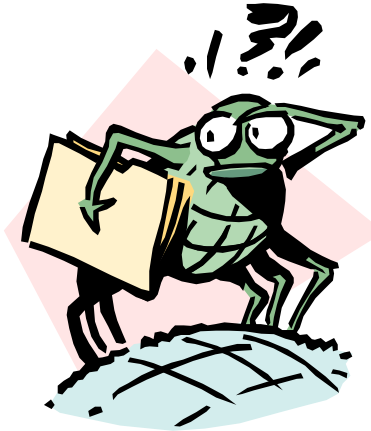
SIS' utvalgte trusler

- Phishing og scam
- Web bugs og spyware
- Identitetstyveri
- Utsiktede menneskelige feil
- Utro tjener
- Misbruk av virksomhetens ressurser
- Tap av mobile enheter
- Single-point-of-failure
- Tjenesteneking
- Datainnbrudd
- Misbruk av trådløs kommunikasjon
- Sikkerhetshull i programvare – standard og spesialutviklet
- Virus og ormer
- Ukritisk bruk av e-post
- Spam
- Hurtigmeldinger og pratekanaler

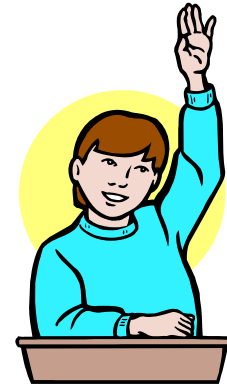


Oppgave

- Hvilken trussel ville du ha rangert på topp?



”Løsning”



- Vanskelig å rangere truslene
- Avhengig av
 - hvilke systemer det gjelder
 - hvor god risikostyring man har
 - hvilke beskyttelsesmekanismer som er i bruk
 - hva man ønsker å beskytte
- Mye sett i Norge:
 - tap av tilgjengelighet
 - utilsiktede hendelser

Trender

- Spam
 - Vil fortsette å øke i mengde
 - Vil også komme nye metoder for filtrering
- Ondsinnet programvare
 - Fortsatt det mest utbredte problemet
 - Vil også ramme mobile enheter som PDA og mobiltelefoner, samt chatte-programmer som MSN og ICQ
- Driftsutsetting av IT-tjenester
 - Forekommer stadig oftere
 - Rutiner og avtaler må forbedres

Mørketallsundersøkelsen 2003

- om datakriminalitet og IT-sikkerhet

Hvorfor?

- Hvilke **typer datakriminalitet** forekommer, og i hvilket **omfang**?
- Er noen **bransjer** mer utsatt enn andre?
- Hvilke **følger** får datakriminalitet?
- Hvor **sårbare** er norske virksomheter på IT-siden?
- Hvilke **sikkerhetstiltak og –rutiner** er satt i verk, og hvordan påvirker det omfanget av datakriminalitet?



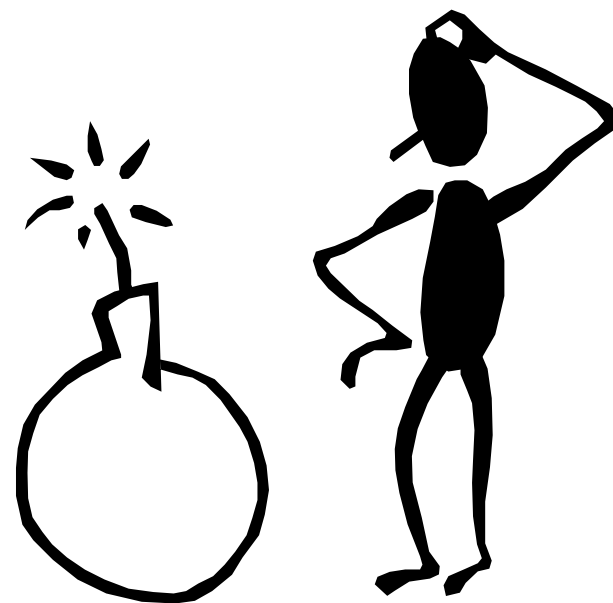


Hovedresultater

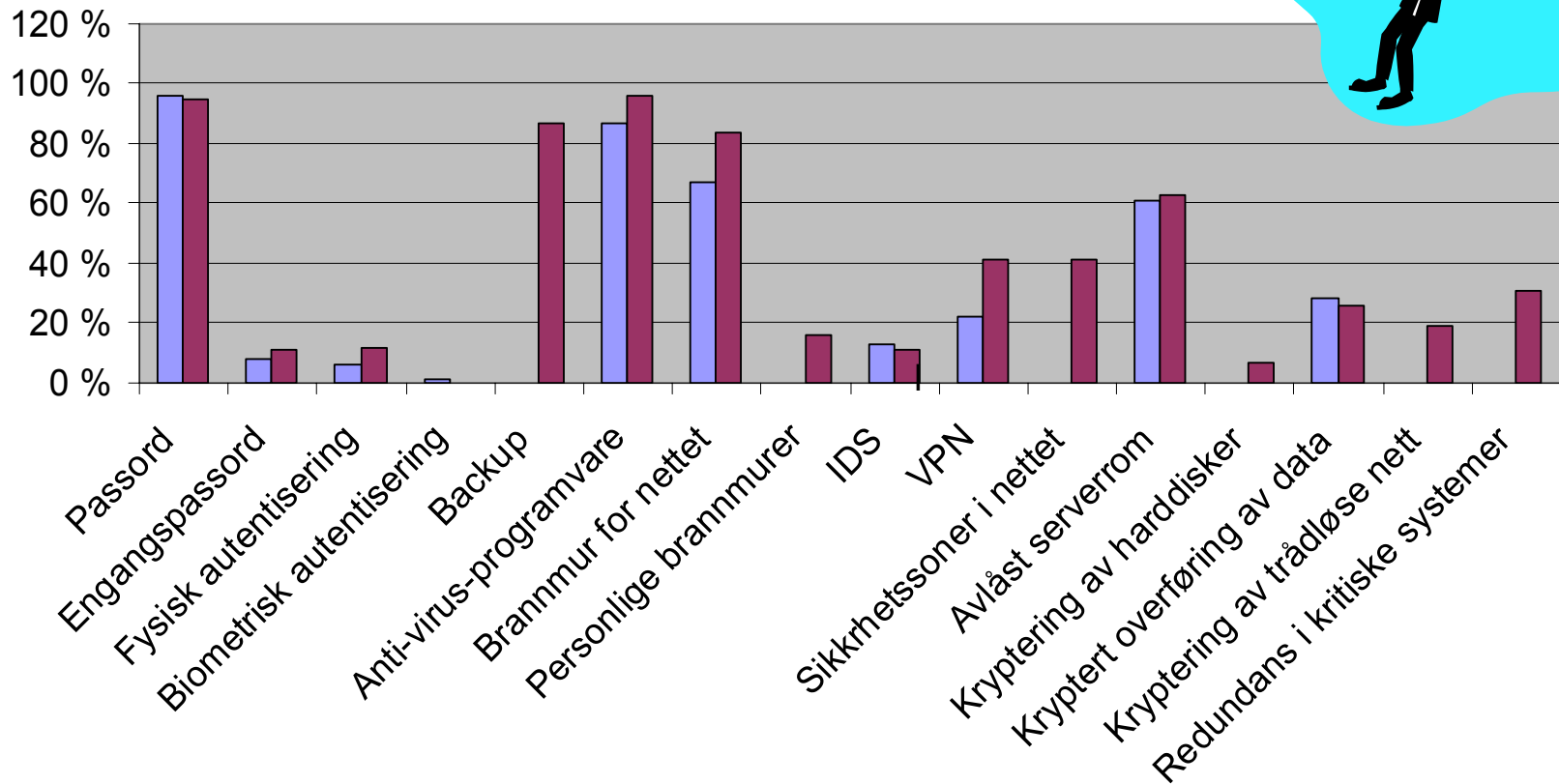
**60% av virksomhetene
er rammet**

Men...

- bare 187 tilfeller er anmeldt
- bare 12 % har rutiner for å estimere tap



Sikringstiltak



Oppdagelse av hendelser

- Bare 44 % går systematisk gjennom logger
- Kun 11 % bruker IDS
- Mer enn halvparten mangler rutiner for å rapportere sikkerhetshendelser internt



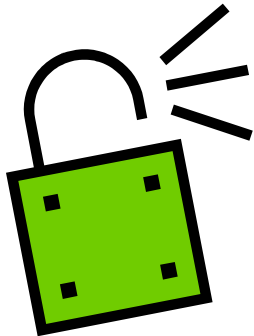
Bank- og finans:

→ 20 % vet ikke om de har vært utsatt

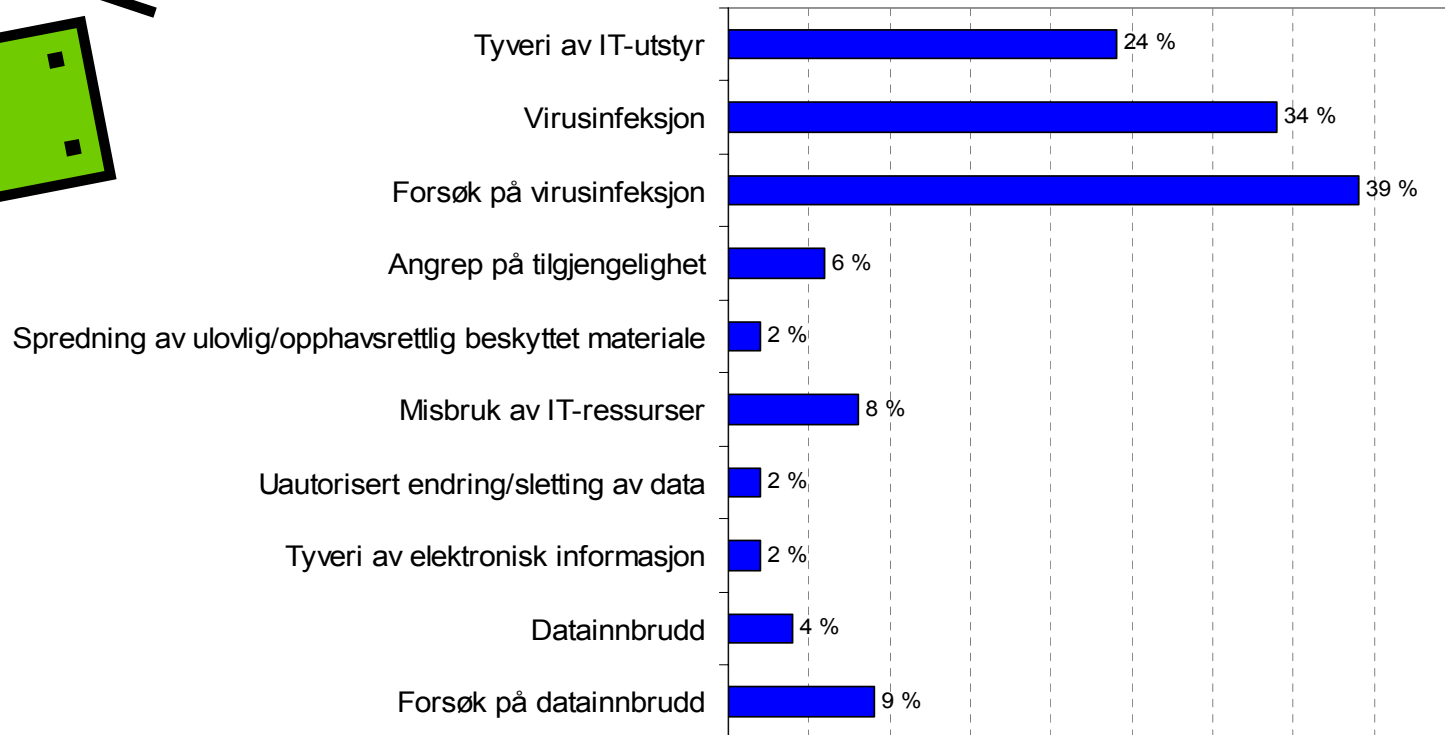
Helse- og sosial:

→ 50 % vet ikke om de har vært utsatt

Omfang av datakriminalitet



60% av virksomhetene er rammet



Eksempler fra media

Dagbladet 2. okt. 2003:

”Norge er virusversting”

→ Er nummer ni på lista over de verste virusspredene i verden regnet per Internett-bruker

Dagbladet 16. juni 2004:

”Økokrim stoppet fildeling fra NetCom-server”

→ Utstyr hos NetCom utnyttet til å spre piratkopiert film og musikk

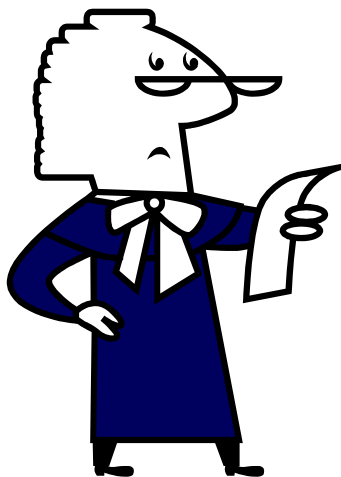
digi.no 24. juni 2004:

”Internett-tekniker solgte adresser til spammere”

→ Ansatt hos USAs største internettleverandør hadde stjålet adresser til over 50 millioner kunder

Gjerningsperson

- Kun 20 % av virksomhetene har klart å identifisere en eller flere gjerningsmenn
- Like ofte egen ansatt som ekstern person

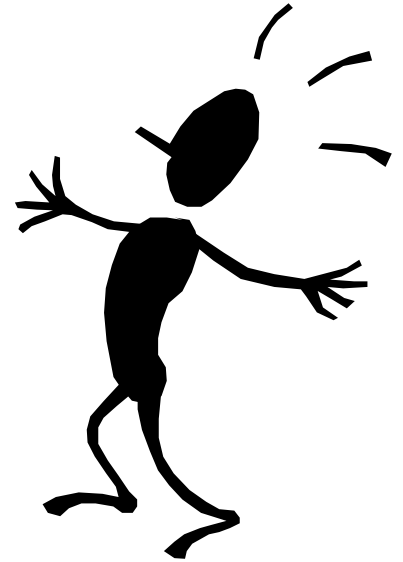


- Tiltak mot gjerningsmann:
 - Oppsigelse
 - Erstatningskrav
 - Sivil sak

Hva er konsekvensene?



Ingen vet kostnaden!



- Bare 25 % er i stand til å anslå direkte tap.
- Bare 6 % er i stand til å anslå indirekte tap.
- Bare 12 % har rutiner for å estimere tapet.
- Ekstra arbeid er den tydeligste konsekvensen.

→ 40 % gjennomgår sikkerheten i virksomheten etter å ha opplevd uønskede hendelser.

Til oppsummering

- **Mørketallene er store!**
 - 5200 datainnbrudd
 - 50 anmeldelser av datainnbrudd
- **Hva er kostnadene???**
- **Stort forbedringspotensiale**
 - Sikkerhetsoppdateringer
 - Trådløse nett
 - Backup
 - Gjennomgang av logger
 - Rapportering internt og eksternt

SIS varslingsstjeneste

- Send e-post til norsis-list@norsis.no
 - med tittel “join sis-varsel@norsis.no” og tomt innhold
 - og få informasjon om nye sårbarheter
 - med tittel “join sis-info@norsis.no” og tomt innhold
 - og få informasjon om oppdateringer på SIS sin nettside
 - nyheter
 - veiledninger
 - månedlige oppsummeringer
 - etc...

Takk for oppmerksomheten!



SIS

SENTER FOR
INFORMASJONSSIKRING

www.norsis.no

post@norsis.no



2004-11-26

www.norsis.no

SIS' utvalgte trusler

Trusselbeskrivelser



Phishing og scam

Sårbarhet:

- Lure til seg sensitiv informasjon eller penger
- Nigeriascam: Lovnad om store penger, men må bidra med litt selv først
- Phishing: Falsk e-post fra virksomhet der du blir bedt om å oppgi sensitive opplysninger
- USA: 50 % økning av phishing hver måned

Tiltak:

- Dersom noe synes for godt til å være sant, er det som oftest det...
- Sjekk med andre kilder
- Vær skeptisk til lenker og annen kontaktinformasjon som kommer på e-post
- Følg med på adresser til nettsteder du besøker



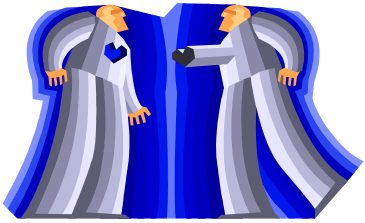
Web bugs og spionprogrammer

Sårbarhet:

- Spionprogrammer lagrer informasjon om surfevaner
- Spionprogrammer endrer nettleser-konfig
- Web bugs i spam bekrefter at adressen er gyldig
- Farlige spionprogrammer
 - Registerer personlige data (navn, kontonummer) og passord

Tiltak:

- Vær kritisk til programvare du laster ned
- Skru av visning av HTML i e-post
 - Alternativ:
Skru av lasting av bilder
- Skru av cookies og aktiv skripting
 - Alternativ:
Slett cookies automatisk



Identitetstyveri

Sårbarhet:

- Misbruk av personopplysninger
- Ofte økonomisk vinning som mål
- Spor overalt: e-post, nettbank, IRC, mobiltelefon, kredittkort
- Falske stillingsannonser
- "Dumpster diving"
- Kredittkort i en annens navn

Tiltak:

- Vern om personopplysninger
 - Både på papir og i elektronisk form
- Vær forsiktig med å legge igjen visse typer informasjon på nettet
- Kryptert kommunikasjon



Utilsiktede menneskelige feil

Sårbarhet:

- Utilsiktede hendelser dominerer
- Komplekse løsninger
- Manglende retningslinjer
- Dårlig etterlevelse
- Manglende risikoanalyse
- Ledelse - hva ønsker de egentlig!?

Tiltak:

- Risikoanalyse
- Øke sikkerhetsbevisstheten
- Klare regler, rutiner og retningslinjer
- Tydelige rapporteringsveier
- Ledelsen må være gode forbilder



Utro tjenere

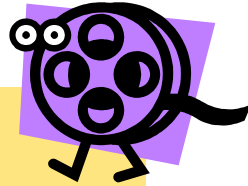
Sårbarhet:

- Misbruk av tillit og tilgang til bedrifts-informasjon
- Ved oppsigelse eller skifte av jobb
 - ..eller fra begynnelsen av

Tiltak:

- Overvåking av interne nett
- Beskyttelse av enkeltmaskiner
- Tilgangskontroll
- Bakgrunnssjekk ved ansettelse
- Tydelig regelverk
 - Muliggjør rettslig forfølgelse

Misbruk av virksomhetens ressurser



Sårbarhet:

- Bruk av ressurser til privat forretningsvirksomhet
- Nedlasting av filer for privat underholdning
 - Lagring og/eller distribusjon
- Fildelingsprogrammer øker faren for ormer/virus
- Uklare grenser
 - hva er lov X hva er ikke lov

Tiltak:

- Tydelige retningslinjer
- Holdningsskapende arbeid
 - Kontinuerlig
- Jevnlige kontroller kan være nødvendig

Tap av mobile enheter



Sårbarhet:

- Enorm utbredelse, folk mye på farten
 - Bærbare PCer, PDAer, mobiltelefoner
- Mye informasjon tapes
 - I tillegg til utstyret i seg selv
 - Bedriftsinformasjon, tilbud, presentasjoner, avtaler
 - Personlige sertifikater, passord, annen personlig informasjon
- Ikke oppdatert policy
 - Mobil hverdag krever mobil sikring

Tiltak:

- Pass godt på alle "dingser"!!
- Sikkerhetslenke på bærbar PC på pulten
- Adgangskontroll til lokaler
- Kryptering
- Sikkerhetskopi av data
- Tilgangskontroll
- Vær bevisst på hva slags informasjon som lagres på en mobil enhet



Single-point-of-failure

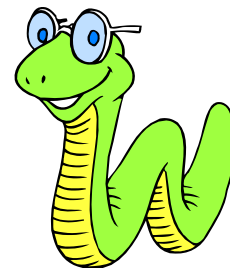
Sårbarhet:

- Stor avhengighet av IT-tjenester og Internett-tilgang
- Ikke reflektert i avtaler med ISP-er
- Redundans i egen infrastruktur
- Backup
- Omlegging av IT-tjenester

Tiltak:

- Still krav i avtaler med ISP
- Jevnlig risikovurdering
- Kontinuerlig oppgradering av teknologi og rutiner
- Dokumenterte beredskapsplaner
- Redundans i infrastruktur

Tjenesteneking



Sårbarhet:

- Ikke planlagt nedetid
- For lite båndbredde
 - Tåler ikke trafikk-mengder utover forventet pågang
- Målrettede angrep
 - Spam, virus
 - DoS-verktøy

Tiltak:

- Sikkerhetsoppdatering/patching
- Høy nok båndbredde
- Redundans
 - Sikre single-point-of-failure

Datainnbrudd



Sårbarhet:

- Sikkerhetshull
- Verktøy utnytter kjente svakheter
- Sosial manipulering
- “For moro skyld” → industrispionasje

Tiltak:

- Sikkerhetsskanning
- Gjennomgang av installert programvare
- Patching, patching, patching!
- Perimetersikring
 - IDS
 - Pakkefilter (brannmur)



Misbruk av trådløs kommunikasjon

Sårbarhet:

- Åpne, trådløse nettverk er hverdagen
 - kafeer, hotell, flyplass, bensinstasjon
- Sikkerhetspolicy utdatert
- Mange virksomheters trådløse nett ikke tilstrekkelig sikret
- Nettverkseieren er den skyldige dersom andre misbruker nettet
 - Hvordan bevise uskyld?

Tiltak:

- Slå på sikkerhetsfunksjoner
- Krypterte forbindelser
- Skepsis til andres åpne nett
- Dynamisk generering av krypteringsnøkkel
- Skjult nettverksnavn
- VPN
- Brannmur og antivirus-program



Sikkerhetshull i standard programvare

Sårbarhet:

- Antall virus og ormer eksplodert
- Kort tid mellom sårbarhet gjøres kjent og angrep kommer
- Patching tar for lang tid

Tiltak:

- Sikkerhetsoppdateringer bør installeres så raskt som mulig
- Hvis tilstrekkelige ressurser: test oppdateringen først
- Alternativt: enkle konfigurasjonsinnstillinger kan avverge angrep eller begrense omfang

Sikkerhetshull

i spesialutviklet programvare



Sårbarhet:

- webapplikasjoner dominerer
- kort "time to market"
- oppretting vanskelig når finansielle transaksjoner er involvert

Tiltak:

- Risikovurdering må gjennomføres før utvikling og før implementering
- Testing, testing, testing...
- Tenk gjennom tiltak for oppretting
- Vurder forsikringsløsninger



Virus og ormer

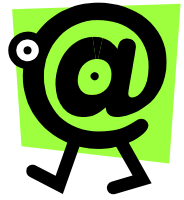
Sårbarhet:

- Via e-post
 - meldingen selv eller vedlegg
- Kopierer seg til kataloger med delte filer
 - "Netsky", "Zafi"
- Chat-programmer
 - "Bizex"
- Kopierer seg til "interessante" filer/kataloger
 - "Netsky", "MyDoom"
- Sikkerhetshull i programvare
 - "Blaster", "Sasser"

Tiltak:

- Antivirus-programvare
 - Alltid oppdatert!!
- Virusskanning av all e-post
- All programvare bør alltid være oppdatert
 - Ikke bare antivirus...
- Vær forsiktig med vedlegg
 - Slett hvis du er usikker
 - Se etter doble filendinger
- Unngå automatisk visning av både e-post og vedlegg

Ukritisk bruk av e-post



Sårbarhet:

- E-post framfor papir
- Mangel på loggføring og arkivering
- Juridiske forpliktelser
- Alle får ansvar for vurdering av om noe er arkivverdig eller ikke

Tiltak:

- Retningslinjer
 - for sending av bedriftssensitiv info
 - for å redusere risiko forbundet med e-post
- System for logg/arkiv
- Visuell kontroll før sending av e-post



Spam

Sårbarhet:

- Lett å samle mange e-postadresser
- Lave kostnader ved utsending
- Forveksling mellom spam og legitim e-post
- MessageLabs: 84 % spam august 2004
- Økende

Tiltak:

- Beskytt e-postadresser
- Unngå å bli misbrukt som formidler av spam
- Antispam-program

Hurtigmeldinger (IM) og pratekanaler



Sårbarhet:

- Bruk av IM i virksomheter forventes å overgå e-post
- Mange virus-infeksjoner via IM
- Gratis IM-tjenester: tjenere utenfor virksomhetens kontroll
- Kommunikasjon i klartekst

Tiltak:

- Retningslinjer for hvilken type informasjon som er tillatt på IM
- Begrensninger på type klient
- Bruk sikkerhetsmekanismer i IM-programvare