
Effektiv håndtering av
sikkerhetspolicies
syscom

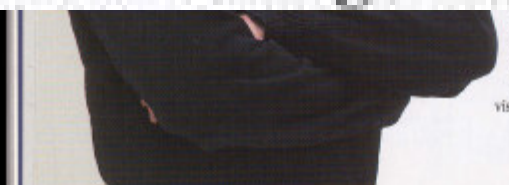
Mennesker, prosess, teknologi..

...according to syscom

...according to

syscom

Det brukes stadig mer penger på oppgradering av norske virksomheters sikkerhetsløsninger. Trusselbildet blir daglig forverret, og for de fleste IT-sjefer blir løsningen å oppgradere brannmur, installere IPS, investere mer i antivirus og antispam, etc. For mange er dette trolig bort i mot bortkastet, med mindre de samtidig satser minst like mye på opplæring av brukere. Selv den sikreste IT-infrastruktur er lite verd dersom brukere lures til å gi fra seg passord og krypteringsnøkler. I følge Gartner er antall Phishing-angrep økende, og disse blir stadig mer spesialisert og målrettet.



i forbindelse med I Love You-viruset, hvor langt over halvpartene klikket på vedlegget selv om de viste at dette var et virus. På

nende forsøk på stjele sensitiv informasjon er å bruke penger på opplæring og holdingsarbeid, og på den måten oppgradere brukerne våre til en ny og sikrere versjon.

espen.hult@idg.no

Hva er den største risikoen i forhold til informasjonssikkerhet?

- 60% av alle hendelser skyldes interne brukere
  - Ansatte gjør utilsiktige feil,spesiellt i forhold til IT
  - Ansatte foretar ulovlilgheter og kriminelle handlinger både bevisst eller ubevisst
  - Innleide, konsulenter eller samarbeidspartnere som ignorerer policies eller har dårlig sikkerhet
- 25% av hendelsene skyldtes malware (ormer, spyware, virus og phising)
- 5% er ulykker som skyldes eksterne forhold
- Mindre enn 5 prosent skyldtes innbrudssforsøk
- MIndre enn 5 prosent av innbruddene var et reellt angrep direkte mot bedriften (mao 0,25%)

- Hvor skal vi legge ned kruttet ?

Tiltak i forhold til risiki!

- Nedetid på systemene som skyldes menneskelige feil medfører mer enn 80 % av all nedetid

- Denne bedriftens anbefaling:
  - Innføring av driftsmessige rutiner basert på ITIL
  - Innføring av prosesserer tilpasset din bedrift/ organisasjon
  - Opplæring i begreper og rutiner for alle i IT avdelingen
  - Innføring av konfigurasjonsdatabase og endringsprosesser
  - Rapportering

Involvering

...according to syscom

Suksessfaktorer

- Involver ledelsen
- Involver brukere i utarbeidelse av policies, oppgraderinger, implementeringer, design mm
- Etabler klare roller og ansvarsområder
- Vær ærlig på hvor problemene og er!

IT SIKKERHET: Orden i huset SIDE 12 OG 13 | Beskytt deg selv SIDE 14

COMPUTERWORLD NORGE NR. 31 • FREDAG 24. SEPTEMBER 2004 SIDE 11

Nå er det flere levende døde

Antallet såkalte zombie-pc-er øker dramatisk. En zombie, eller bot, er en orme-befengt pc som kan styres av hackere og brukes til fiendtlige angrep på andre datamaskiner. De infiserte maskinene kobles sammen i såkalte botnet.

I januar oppdaget sikkerhetsselskapet Symantec 2.000 zombie-maskiner daglig, ifølge The Register.

I sommer var tallet steget opp til 30.000 per dag, med 75.000 som er foreløpig rekord. *(AS)*

Skrev virus, fikk jobb

Sendte sjefen på kurs

Forankrer it-sikkerhet i toppledelsen

Da rederiet Wallenius Wilhelmsens fikk ny konsernsjef, måtte han på kurs hos it-sikkerhetsansvarlig John Arild Johansen.

ARNE SØILAND

— Begynn med toppledelsen. Skrem dem med eksempler fra bedrifter som ikke har tatt it-sikkerhet på alvor. Samtidig må du sørge for å ha en plan for å sette i verk de nødvendige tiltakene, sier John Arild Johansen.

Johansen er ansvarlig for it-sikkerhet i Wallenius Wilhelmsen. Det norsk-svenske rederiet, eid av Wilh. Wilhelmsen og Wallenius Lines, har 3.000 ansatte på fem kontinenter. I fjor fraktet rederiets skip over to millioner biler til sjøs, mens 1,5 millioner biler ble fraktet langs

FOTO: ARNE SØILAND

HØYT OG LAVT: – Sikkerhetssjefen må være en god markedsfører, samtidig som han skjønner forretningsprosessene, sier John Arild Johansen, it-sikkerhetssjef i Wallenius Wilhelmsen.

gjengelighet, som er målene i alt it-relatert sikkerhetsarbeid.

om hva gjentatte brudd på reglene vil føre til.

De menneskelige truslene mot it-sikkerhet dreier seg ikke bare om å åpne virusbefengte vedlegg, eller å bruke for enkle passord. Sosial manipulering, altså at folk kommer inn i bedriften og utgir seg for å være andre enn de er, begynner også å bli mer utbredt.

Hos Wallenius Wilhelmsen har man leid inn folk som fikk i oppgave å drive sosial manipulering for å få tak i informasjon. Heldigvis lyktes de ikke. Det kan tyde på at rederiet har gjort noe riktig, uten at det gir grunn til å hvile på laurbærene.

Kontinuerlig markedsføring er

FOTO: WALLENIUS WILHELMSEN

KRITISK: Wallenius Wilhelmsen er et av verdens største rederier innen transport av biler og andre kjøretøyer.

viktig. It-sikkerhetssjefen må være synlig.

— Jeg hadde ikke hatt nubbtjangs uten å skrike og høje overalt, understreker John Arild Johansen.

ARNE SØILAND/COMPUTERWORLD.NO

Informerer alle ansatte

Alle ansatte i Wallenius Wilhelmsen mottar denne teksten fra konsernsjef Nils P. Dyvik:

«Sikring av informasjonseiendelene:

Vi må erkjenne at det de siste årene har vært en betydelig økning i verdien av og tilgjengeligheten av informasjon og data, som medfører økt en risiko for informasjonssikkerheten.

Vi må ta de potensielle risikoene knyttet til verdien av bedriftsinformasjon svært alvorlig.

De teknologiske fremskrittene de seneste årene har resultert i en ny informasjonskultur.

Det er derfor nødvendig fastsette dertil egnede tiltak for å beskytte mot det økende antallet risikoer for informasjonssikkerheten.

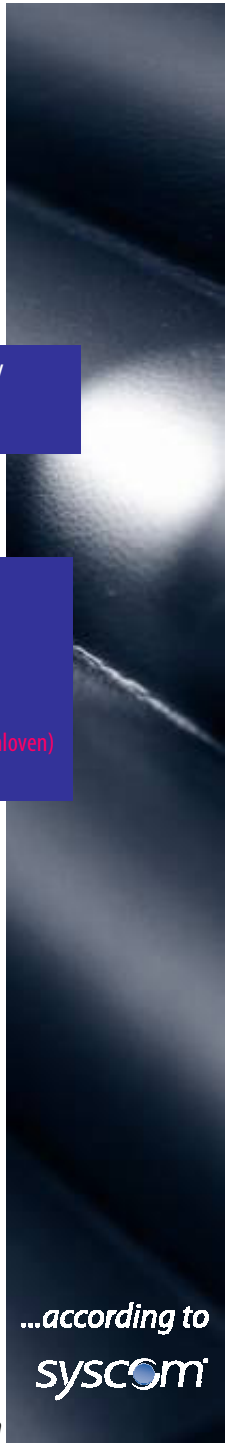
Det er påkrevd at alle ansatte og alt innleid personell støtter denne prosessen og omhyggelig etterfølger gjeldende informasjonssikkerhetsregler og — veiledninger, slik at det er mulig å garantere et tilstrekkelig sikkerhetsnivå for våre informasjonseiendeler.»

konfidensialitet, integritet og til- ge. Regelverket må gi klar beskjed

"Rammeverklandskapet" for security policies

Prinsipp basert	Kontroll basert	Revisjons guider	Security metrics	Mgt guides	Sektor baserte	IT Govern / Mgt	Lovverk/ regler
OECD Guidelines GAPP GAISP NIST 800 NIST 800-14 NIST 800-26 NIST 800-27 IFAC	BS 7799 ISO 17799 AICPA SGPIS ITCG ISO TR 13335 BSI NIST 800-12 NIST 800-37 NIST 800-53 PIPEDA EU DPD FDA 21 CDR DTI	FISCAM SAC IIA RF eSAC IIA RF	NIST 800-55 CBST	CSGSM ISA IS for Execs	ISG 1200 Basel II ISO TR 13569 BITS FFIC	ITGI CoBIT **ITIL**	SOX GLBA HIPAA CA SB FTC guide (Personvernloven)

Kilde: Comitee on Government Reform



Sikkerhetsintruks

AVTALE OM BRUK AV DATASYSTEMER OG BEHANDLING AV PERSONOPPLYSNINGER

Regler for IT-brukere gjelder for alle ansatte, alt innleid personell og andre som gis tilgang til bedriftens IT ressurser, i eller utenfor Bedriftens lokaler.
Regler for IT-brukere gjelder også bruk av bedriftens IT-systemer gjennom oppkobling med privat IT-utstyr eller utstyr som omfattes av Bedriftens "hjemme PC" avtale.

Som medarbeider i Firmaet behandler du forskjellige former for data, dette kan også dreie seg om opplysninger av sensitiv og fortrolig art ellerforretningshemmeligheter. Det er derfor påkrevd med gode og strenge sikkerhetsrutiner for å ivareta en høy grad av sikkerhet. Dette gjelder både ved lagring internt, tilgang til systemet og ekstern overføring. Hensiktsmessig personaladministrasjonen og administrasjon av IT ressurser i Firmaet nødvendiggjør også til en viss grad behandling av personopplysninger om den enkelte.

Disse opplysningene skal håndteres i henhold til Datatilsynets retningslinjer.

Denne instruks og avtale gjelder bruk av Firmaets datasystemer og Firmaets behandling av personopplysninger, og vedlegges ansettelsesavtalen.

Denne bestemmelse er ikke til hinder for at den enkelte, også etter at arbeids- eller oppdragsforholdet er avsluttet, rettmessig skal kunne nyttiggjøre seg ervervet alminnelig kunnskap, ferdighet og erfaring i henhold til bestemmelseri ansettelsesavtalen.

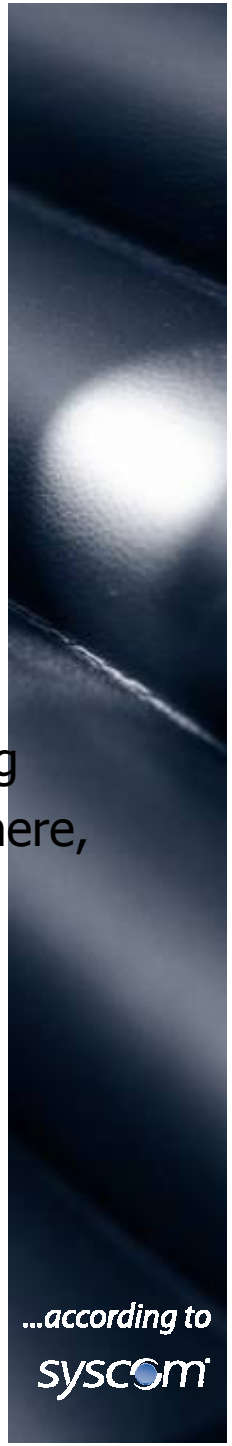
....
Navn (blokkskrift) Dato, underskrift

Avtalen/instruksen signeres og sendes nærmeste overordnede leder, eventuelt personalarkiv, for oppbevaring sammen med ansettelseskontrakt.

Sikkerhetsinstruks...

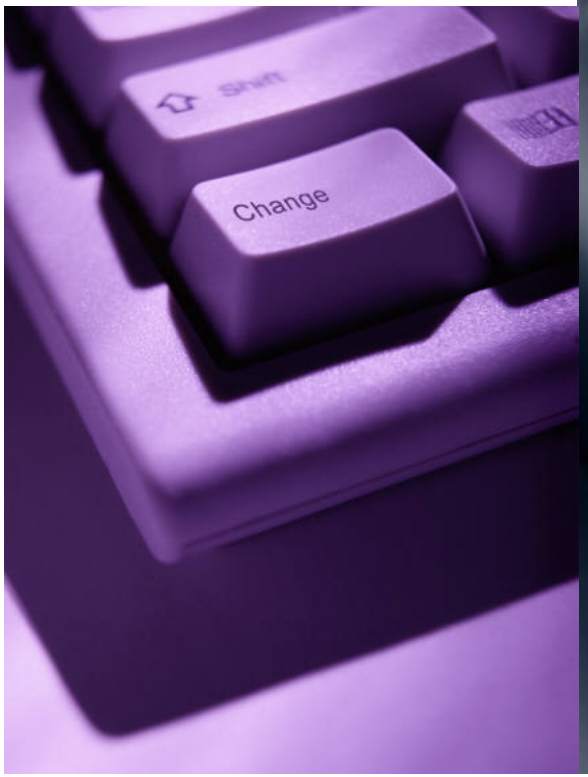
Regler for IT-brukere

- Bruk av data til private formål
- IKT-utstyr må godkjennes
- Surfing og bruk av tjenester på internett
- Passord og tilgang
- Dokumentsikkerhet
- Bruk av mobiltelefoner og PDAer
- Sikring av maskiner
- Ekstern påkobling
- Innsyn
- Registrering av aktivitet /logging
- Bruk av IT hos samarbeidspartnere, foretningsforbindelser kunder
- Skanning
- Årlig revisjon, endringer mv
- Konsekvenser ved brudd



6 ting du bør tenke på

- Sikkerhetspolicies
  - Definer etterlevelse og sanksjonsmuligheter
  - Avklar revisjon og evaluering
  - opplæring og kultur
- Endringer
  - Kartlegg hvordan du håndterer endringer
  - Hva innebærer en endring i ditt miljø
  - Hvem avgjør hvilke endringer som skal utføres når
- Informasjonssikkerhet
  - Lag en oversikt på de lover og regler som er relevante for din virksomhet
  - Avdekk hvilke fremtidige krav står du overfor



6 ting...

- Emergency
  - Hvilke sannsynlig scenario er ”worst case” for deg ?
  - Hvis krisen oppstår: hvem - hva – hvordan - når
  - Ekstern kommunikasjon
- Lovbrudd
  - Hvis en av dine ansatte begår et lovbrudd med virksomhetens IT utstyr, hva gjør du da?
  - Etterforskning
- Ny Teknologi
  - Hva er konsekvensen

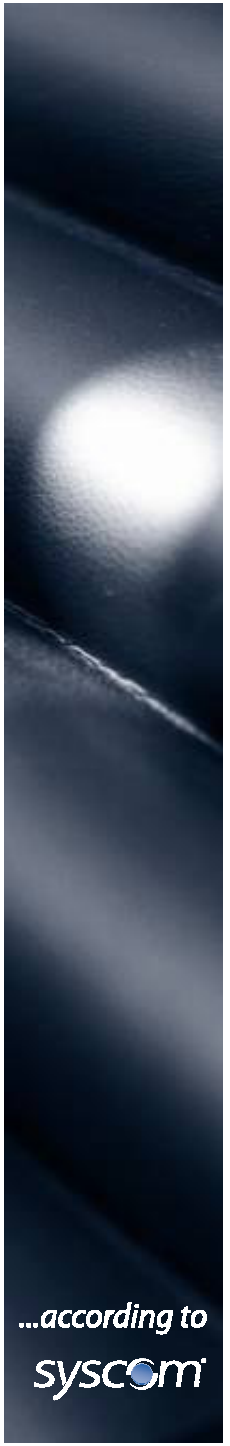
...according to syscom

Verktøy

...according to syscom

Verktøy for rapportering av sikkerhetsnivå

- Endpoint compliance
  - Viruskontroll, Authentisering, Kryptering, Patchkontroll, Personlig Brannmur m. fl
  - Validerering av utstyr og maskiner ut fra sikkerhetspolicy
  - Tilgangskontroll av brukere
  - Karantenenett
    - Symantec, Sygate, LANDesk, Juniper Networks m. fl
- Rapportering av sikkerhetshendelser
  - Security Incident management (SIM)
  - Logghåndtering i relasjon til brukeratferd, trusselbilde
  - Avvikshåndtering av bedriftens policy
    - Arcsight, Netforensics, IBM, Symantec m. fl
- Policy Compliance
  - Rapportering i henhold til definerte standarder; ISO 17799, BS7799, HIPAA, Basel II, Sarbannes Oxley
    - Symantec, Arcsight m. fl



Oppsummering

- Involvèr og skap forståelse hos
  - Ledelsen
  - Brukere
- Utarbeid gode rutiner for endringer
  - ITIL
- Security Management av infrastruktur
  - Verktøy
  - Compliance til eksterne krav og regler

?

gs@syscomworld.com

Mob 918 51251

www.syscomworld.com