Norske bedrifter uten kontroll på sensitive data

De fleste norske bedrifter slurver med å beskytte sensitiv informasjon eller personopplysninger på data. Det viser en fersk undersøkelse Perduco har gjort for Jussystemer.

Halvparten av næringslivslederne kjenner ikke til lovene de er pålagt å følge i forbindelse med håndtering av personopplysninger. Norske bedrifter ligger dermed vid åpne for alle som ønsker å hente sensitiv informasjon eller personopplysninger.

Vedlagt:
- *Funn fra undersøkelsen*
- *Hva bør daglig leder gjøre for å sikre et minimum av sikkerhet?*
- *Hva bør ansatte vite om informasjonshåndtering og sikkerhet*

Hele undersøkelsen finner du her:

Noen hovedfunn fra undersøkelsen:

Perducos næringslivspanel, 1259 næringslivsledere fra hele landet. Undersøkelsen ble tatt opp i slutten av november.

- To tredeler sender e-post ukryptert
- 40 prosent av norske bedrifter har ikke regler for håndtering av sensitiv bedriftinformasjon
- Kun 4 prosent i industrinæringen sender kryptert e-post
- Kun halvparten av de spurte kjenner de juridiske og rettslige konsekvensene av av brudd på personopplysningsloven med forskrift
- 14 prosent sier de har mottatt feilsendte e-poster med sensitiv informasjon og/eller personalopplysninger, 4 prosent sier de har sendt slik e-post selv

- Hvis du sender en epost utenfor brannmuren der du jobber, vil den på sin ferd mot mottageren foreta flere stopp i det åpne internettrommet på servere rundt i verden. Her kan mailen din leses, informasjon sorteres og lagres. Om og når det eventuelt brukes vet du ikke, sier Audun Høisæther, sikkerhetsekspert hos Jussystemer AS.

Lett å få tak sensitiv bedriftsinformasjon
Sensitiv bedriftsinformasjon blir stadig lettere å få tak i. Næringslivsledere, finansfolk og kommunikatører sender åpne e-poster, går rundt med usikrede PCer i sekker og vesker, legger igjen usikrede datamaskiner på flyplasser og i taxier og legger igjen usikrede minnepinner med viktig informasjon overalt. Dette er meget betenkelig, da det ofte handler om børssensitiv informasjon, strategier, nye produkter eller personopplysninger.

Sist uke måtte lederen i et britisk institutt for klimaforskning gå av etter en internasjonal skandale: Uvedkommende fikk tak i flere tusen e-mail mellom fremtredende forskere på feltet. Dette viser at e-poster og viktig informasjon er tilgjengelig hele tiden. Norske næringslivsledere ser ifølge undersøkelsen likevel ikke ut til å bekymre seg.

For ytterligere informasjon eller kommentarer, kontakt Audun Høisæther, datasikkerhetsekspert hos Jussystemer, på mobil 900 72 229.

Hva bør daglig leder gjøre for å sikre et minimum av sikkerhet?

Sikkerhetsråd fra Audun Høisæther i Jussystemer

For å sikre et minimum av sikkerhet ville jeg som daglig leder ha gjort følgende:

1. **Kartlegging**
   Jeg ville ha gjennomført en kartlegging over hvilken informasjon vi enten hentet inn, behandlet og lagret. Jeg ville ha sett både på personopplysninger og kritisk/sensitiv bedriftsinformasjon.

2. **Lovpålagte krav**
   Jeg ville på grunnlag av kartleggingen ha avklart om mitt firma var underlagt for eksempel Personopplysningsloven m/forskrift. I så fall ville styret være eksponert, og det er min plikt som daglig leder å sikre at selskapet driver i henhold til norsk lov.

3. **Hvordan lagrer og distribuerer vi informasjon?**
   Dette ville jeg ha sett i forhold til:
   - **a.** Server
   - **b.** Filer/mapper
   - **c.** E-post
   - **d.** USB
   - **e.** CD
   - **f.** Mobil
   - **g.** Bærbart utstyr
   - **h.** Kopiering/scanning

4. **Eksponering**
   Jeg ville ha sett på kritiske punkter for eksponering for uautorisert innsyn, dvs hvem kan potensielt få tilgang til våre data:
   a. Hvordan håndterer vi elementene nevnt i pkt. 3
   b. Har alle på IT tilgang til all informasjon som lagres?
   c. Hvilke ansatte har tilgang ellers?
   d. Kan utenforstående få tilgang?

5. **Fjerning av data**
   Jeg ville hatt klare retningslinjer for hvor lenge data lagres og hvordan data slettes/fjernes, herunder også hvordan vi behandler gammelt utstyr ved kjøp av nytt. Nevnes her kan PC (både stasjonært og mobilt), kopieringsmaskiner, mobiler og alt utstyr som lagrer informasjon.

6. **Opplæring av ansatte**
   Uten at ansatte er med på laget har man svakt sikkerhetsnivå.

Hva bør ansatte vite om informasjonshåndtering og sikkerhet:

1. **Retningslinjer/policy for informasjonshåndtering**
   Lage overordnede retningslinjer/policy for behandling av informasjon, både personopplysning og kritisk/sensistiv bedriftsinformasjon. Dette ville jeg hatt styrebeslutning på.
2. **Instrukser/rutiner for å understøtte pkt 1 over**
   Instruks for bruk av internett, e-post, USB, CD osv
3. **Etiske retningslinjer**
   Jeg ville hatt etiske retningslinjer som omfatter behandling av informasjon, herunder hvilke regler som gjelder for taushet og konfidensialitet.
4. **Opplæring**
   Dette er kritisk. Jeg ville hatt skikkelig innføring/opplæring i følgende:
   a. kritiske paragrafer i Personopplysningsloven og forskriften

b. bedriftens retningslinjer, policy og instrukser
c. rutiner for informasjonshåndtering i videste forstand
d. gjennomgang av bedriftens kritiske punkter, hva angår fare for å bli eksponert for uautorisert innsyn

Endelig så ville informasjonssikkerhet stått på agendaen i alle internmøter. Temaet må være varmt hele tiden.

(Audun Høisæther)