NOTAT

26-05-2014

Sagsnr.
2014-0040160

Dokumentnr.
2014-0040160-1

Sagsbehandler
Jesper Klitgaard Jørgensen

Til Økonomiudvalget

Orientering til Økonomiudvalget om IT-sikkerhedshændelser i 2013

Baggrund
IT-sikkerhedsfunktionen i Koncernservice orienterer en gang årligt om konstaterede væsentlige it-sikkerhedshændelser i Københavns Kommune til Økonomiudvalget. IT-sikkerhedsfunktionen informerer samtidig om hvilke tiltag, der er blevet gjort.

Væsentlige hændelser
IT-sikkerhedsfunktionen er bekendt med to væsentlige brud på IT-sikkerheden i 2013. De er beskrevet nedenfor.

Brud 1 – Økonomiforvaltningen – personfølsomdata på kk.dk
I forbindelse med offentligt udbud af en ejendom på Københavns Kommunes hjemmeside under salg af ejendomme er der fremlagt en kopi af en enkelt lejekontrakt, idet ejendommen var udlejet.Ved en fejl får Center for Byudvikling, Afsnit 3 ikke overstreget et cpr-nr. i kontrakten.

Lejeren gør opmærksom på fejlen, og samme dag bliver cpr-nr. slettet fra hjemmesiden.

Den korrekte håndtering af cpr-nr. er blevet præciseret i de interne arbejdsgange.

Sagen er indirekte omtalt i en artikel "Det åbne arkivskab på Herlev" i Jyllandsposten 2. september 2013. Sagen har ingen yderligere konsekvenser haft.

Brud 2 – Socialforvaltningen - manglende pinkode på SIM-kort og adgangskode til enhedens skærmslås
En medarbejder fik stjålet sin arbejdsmobil. Telefonen var opsat med synkronisering af mail (Outlook/Exchange), der indeholdt personfølsomme oplysninger. Telefonen havde ikke pinkode på SIM-kort eller adgangskode til enhedens skærmslås.

Medarbejder kontaktede selv udbyder af SIM-kort for at lukke for opkald. Medarbejder blev bedt om at henvende sig om tyveri til sin egen forvaltning for at afbestille synkronisering. Kendeord blev ændret så synkronisering ikke var mulig.

IT-sikkerhedsfunktionen orienterede medarbejderens leder for at indskærpe, at medarbejdere skal overholde regler for sikring af mobile

enheder herunder at anvende pinkode på SIM-kort og adgangskode til enhedens skærmslås.
Desuden orienterede IT-sikkerhedsfunktionen digitaliseringscheferne i Københavns Kommunen forvaltninger om hændelsen, for at indskærpe at arbejdstelefoner eller andre mobile enheder, der synkroniserer mail skal sikres med pinkode på SIM-kort og adgangskode til enhedens skærmslås.
IT-sikkerhedsfunktionen publicerede også et indlæg på Københavns Kommunes intranet om reglerne.
Regler og vejledninger til at sikre mobile enheder fremgår af kommunens IT-Sikkerhedshåndbog (http://kk-it-sikkerhed/main/policy/collection?colguid=SA13B89E92F2FY3ABU).

IT-sikkerhedsfunktionen har ikke konstateret misbrug af data som følge af hændelsen.

Øvrige hændelser
IT-Sikkerhedsfunktionen har kun modtaget enkelte øvrige indberetninger om mindre IT-sikkerhedshændelser og driftsforstyrrelser.I de tilfælde har IT-sikkerhedsfunktionen samarbejdet med relevante chefer og informeret medarbejdere om regler.

Oftest har hændelserne handlet om, at en chef skal sikre at procedurer og arbejdsgange er tilgængelige for medarbejderne, så de efterlever kommunens IT-sikkerhedsregler.