KØBENHAVNS KOMMUNE
Koncernservice
Forretningsstøtte

NOTAT

Til Økonomiudvalget

01-02-2011

Sagsnr.
2011-15264

Dokumentnr.
2011-77460

Sagsbehandler
Jens Magnild/Brian Thordarson

Årlig indberetning til BR vedr. konstaterede it sikkerhedsbrud.

Orientering om it-sikkerhedsbrud og anbefalinger til forbedringer.

Ifølge § 79. Stk. 5. i Regulativ for it-sikkerhed i Københavns Kommune af 16. december skal It-sikkerhedsfunktionen én gang årligt inden udgangen af 1. kvartal orientere Økonomiudvalget om konstaterede it-sikkerhedsbrud.

Ifølge § 80. *Stk. 3*. i Regulativ for it-sikkerhed i Københavns Kommune af 16. december skal It-sikkerhedsfunktionen mindst én gang om året vurderer, om periodens hændelser giver anledning til forbedringer af it-sikkerheden**.**

Det kan indledningsvist oplyses, at antallet af it-sikkerhedsbrud ikke har ændret sig væsentligt i forhold til tidligere år.

Koncernservice

Ottiliavej 1, 7 sal, 732
2500 Valby

Telefon
3366 5611

E-mail
bt@ks.kk.dk

EAN nummer
5798009809018

www.kk.dk

Anbefalinger til forbedringer:

-

It-sikkerhedsfunktionen er etableret i 2010 i Koncernservice. Der er etableret en større grad af specialisering og ekspertise end man før havde da hver forvaltning havde en egen it-sikkerhedsleder. Denne proces skal fortsættes og udbygges.

Der skal udarbejdes flere fælles opdaterede politiker og retningslinjer på tværs af kommunen.

It-sikkerhedsfunktionen har igangsat en risikoanalyse, som skal færdiggøres med anbefalinger til forbedringer og der skal herefter udarbejdes en ny beredskabsplan.

Kommunens nye internetpolitik skal færdiggøres og markedsføres på KKnet. Det videre forløb aftales mellem It-sikkerhedsfunktionen og med BR-sekretatiatet. Dette vil forebygge en gentagelse af de typer af it-sikkerhedsbrud, som relaterer sig til brug af internettet.

Orientering om it-sikkerhedsbrud:

Personhenførbare oplysninger lækket på Internettet i to forvaltninger:

It-sikkerhedsbrud **BIF**:

It-sikkerhedsfunktionen i KS blev i juni 2010 kontaktet af en ansøger til puljemidler som klagede over at hendes projektansøgning til Det lokale Beskæftigelsesråd, Jobcenter København lå offentligt tilgængelig på Internettet med personidentificerbare oplysninger. Oplysningerne kunne findes på ansøgerens navn på Google. Det samme viste sig at gælde andre ansøgere.
BIF valgte herefter slette alle dokumenter fra det pågældende system (LBR's systemet), og google har slettet alle links og cacher af disse dokumenter.
BIF gik i gang med at finde en ny løsning, som kunne indeholde projektansøgninger på en sikker og hensigtsmæssig måde.
BIF er endvidere blevet bedt om at indføres forretningsgange, som sikrer at lignede data ikke offentliggøres i fremtiden.

It-sikkerhedsbrud i **BUF**:

It-sikkerhedsfunktionen modtog den 5. august 2010 en henvendelse fra

Bellahøj politi. Det var blevet anmeldt, at der var adgang til interne oplysninger om medarbejdere ved kommunen (Børne- og ungdomsforvaltningen) direkte fra Internettet. Via Google kombineret med to andre søgetjenester kunne man uden brugerkode få adgang til et ubeskyttet regneark i BUF på en hjemmeside, som indeholdt navne, personnumre og visse lønoplysninger på omkring 13.000 ansatte. BUF´s ledelsesrepræsentant blev bedt om straks at sikre, at oplysningerne blev fjernet fra Internettet. BUF meddelte senere samme dag, at der var blevet lukket for regnearket.
Da It-sikkerhedsfunktionen foretog kontrol den 9. august 2010 viste det sig at regnearket alligevel ikke var lukket, og BUF blev på ny bedt om straks at fjerne oplysningerne og om nødvendigt kontakte systemleverandøren.
Den 10. august meddelte BUF, at regnearket nu er permanent fjernet af teknikerne og at problemet er løst. BUF har endvidere indskærpet over for medarbejderne, at der ikke må publiceres personoplysninger på websider, der er tilgængelige uden autorisation.
Ved fornyet kontrol var der ikke længere adgang til oplysningerne.
Bellahøj Politi har henlagt sagen.

It-sikkerhedsbrud **KFF.**:

Ulovlig brug af fælleslogin i bibliotekerne:

It-sikkerhedsfunktionen har konstateret:

1. At der bruges ulovlige fælleslogin i samtlige biblioteker ved indlogning på skranker og reference pc`ere, hvilket er i strid med persondataloven, der foreskriver, at man skal logge ind med en personlig brugerident på systemer, der behandler personfølsomme data.

2. At man i mindre udstrækning bruger løst ansatte bogopsættere, hjælpere etc., der ikke er oprettet korrekt via KS Brugeradministration med en unik systemgenereret brugerident eller har underskrevet tavshedserklæring. Det er særligt alvorligt, da de i nogle tilfælde assisterer i skrankerne og dermed bruger fælleslogin og får adgang til lånernes personfølsomme data.

It-sikkerhedsfunktionen har haft møde med bibliotekerne og aftalt at

iværksætte følgende tiltag for at få lovliggjort arbejdsprocesserne:

- KFFs direktion vil via et notat blive informeret om den ulovlige brug af fælleslogin, da de er ansvarlige for at it-sikkerhedsregulativet overholdes i forvaltningen og at man ikke anvender fælleslogin i Bibliotekerne.
- KFF er anmodes inden 1. januar 2010 om enten at stoppe brugen af fælleslogin eller bevilge penge til at indhente et estimat på en biometrisk løsning lavet af KS med eks. fingerscanning til at identificere den enkelte bruger for ca. 100 skranker/reference pc`er. Samt implementerer løsningen.
- 100 testbrugere fra bibliotekerne vil blive tilmeldt næste fase af SSO/VDI projektet, hvor løsningen på langt sigt kan blive implementeringen af en "smart card" løsning.
- Samtlige ledere i bibliotekerne er tilskrevet om problemet med løst ansatte, der er ulovligt oprettet, og der henstilles til, at man omgående sørger for at få alle, der hjælper til i skrankerne, ansat på korrekt vis.
- Til de løst ansatte, der bistår i skrankerne vil der ligeledes blive lavet en tro- og love erklæring, der udsendes fra KFFs HR afdeling sammen med ansættelseskontrakten.

CPR numre på bibliotekernes publikums pc`ere:

Vi konstaterede i foråret, at på visse publikums maskiner hos bibliotekerne kunne alle og enhver ved at gå ind i c/:Documents and settings se en liste med cpr numre på de personer, der tidligere havde været logget ind på pc`en.

Årsagen var et uheldigt samspil imellem 2 programmer: Book-pc, der benyttes på næsten alle biblioteker i dag til bookning på Internet pc`ere, samt Deep Freeze, der sletter alt, hvad den enkelte bruger har lavet på pc`en af søgninger m.m.

Ideen er, at pc`en bringes tilbage til en default tilstand til den næste bruger. På den måde undgår man virus og ophobninger af installerede programmer samt at næste bruger kan se, hvad tidligere brugere har lavet af søgninger samt deres cpr. numre.

Grundet en fejl i et image, virkede programmet Deep Freeze ikke på nogle af maskinerne, derfor blev internetsøgninger samt cpr-numre ikke slettede og lå frit tilgængeligt på pc`ernes c/: drev under documents & settings.

Problemet blev løst inden for ganske få dage efter et samarbejde imellem KS teknikere og de lokale it-ansvarlige ude på bibliotekerne.

Der blev lavet et script, der kørtes på samtlige publikums pc`ere i bibliotekerne (ca. 2000), som fjernede de ophobede data fuldstændigt fra c/:drevet, og de defekte images blev repareret, så det ikke kunne ske igen.

Ved stikprøver i foråret 2010 på bibliotekerne på en del publikums pc`ere er der ikke fundet nogen cpr-numre eller defekt image, så sikkerhedsbruddet er stoppet.

På længere sigt arbejder KS teknikere også på en anden løsning til at øge sikkerheden omkring borgernes persondata på publikums pc`ere.

Sikkerhedsbrud i **SUF**

Print sendes til forkerte printere og skærme:

I marts 2010, bliver It-sikkerhedsfunktionen bekendt med at der kommer dokumenter fra Omsorgssystemet op på skærmen hos brugere, som ikke har noget med printet at gøre og som ikke burde have adgang til Omsorgssystemets data.

Koncernservice's serverdift prøvede at løse problemet og der blev fundet en midlertidig løsning på problemet.

I juni 2010 dukker samme problem op igen. Der er kobles et eksternt firma på, der forsøger at løse problemet. Men ved årets udgang er problemet ikke løst og det eksterne firma arbejdes stadig på en løsning.

Sundhedsforvaltningens direktion er informeret.