KØBENHAVNS KOMMUNE
Økonomiforvaltningen

NOTAT

Til Økonomiudvalget

08-04-2010

Sagsnr.
2010-55472

Dokumentnr.
2010-238859

Sagsbehandler
Jeannette Pautsch

Orientering af ØU om it-sikkerhedshændelser i 2009

Efter § 79, stk. 5, i it-sikkerhedsregulativet for Københavns Kommune skal Borgerrepræsentationens Sekretariat én gang årligt orientere Økonomiudvalget om årets konstaterede it-sikkerhedsbrud. Orienteringen skal ske inden udgangen af 1. kvartal i det efterfølgende år.

It-sikkerhedslederne skal forinden (inden udgangen af årets 4. kvartal) efter § 79, stk. 4 have orienteret vedkommende fagudvalg om konstaterede it-sikkerhedsbrud.

Der er i 2009 konstateret følgende:

- *Borgerrådgiveren*

Ingen it-sikkerhedsbrud

- *Intern Revision*

Ingen it-sikkerhedsbrud

Borgerrepræsenta-tionens Sekretariat

Rådhuset, 2. sal, vær. 12
1599 København V

Telefon
3366 4176

Telefax
3366 7000

E-mail
jmp@okf.kk.dk

EAN nummer
5798009800275

www.kk.dk

- *Økonomiforvaltningen*

2 it-sikkerhedsbrud, se bilag 1 og 2

- *Kultur- og Fritidsforvaltningen*

3 it-sikkerhedsbrud, se bilag 3

- *Børne- og Ungdomsforvaltningen*

1 it-sikkerhedsbrud, se bilag 4

- *Teknik- og Miljøforvaltningen*

4 it-sikkerhedsbrud, se bilag 5

- *Sundheds- og Omsorgsforvaltningen*

Ingen it-sikkerhedsbrud

- *Socialforvaltningen*

1 it-sikkerhedsbrud, se bilag 6

- *Beskæftigelses- og Integrationsforvaltningen*

Ingen it-sikkerhedsbrud

Bilagenes tekst er baseret på de respektive forvaltningers indberetninger til Borgerrepræsentationens Sekretariat.

Bilag 1

It-sikkerhedsbrud i Økonomiforvaltningen 2009

Hændelsen
Fredag den 29. maj 2009 modtog Center for Borgerservice en mail fra Datatilsynet i anledning af, at Datatilsynet havde konstateret, at der på flere lokaludvalgs hjemmesider lå fortrolige personoplysninger. Datatilsynet sendte links til 5 hjemmesider og meddelte, at adgangen til disse hjemmesider øjeblikkeligt skulle fjernes. Der var tale om offentliggørelse af bl.a. personnumre og bankoplysninger på tilskudsansøgere, der i deres ansøgning til lokaludvalgenes puljemidler, har inkluderet oplysningerne i deres ansøgningsmateriale. Materialet var herefter blevet udgivet på Internettet via kommunens dagsordenssystem.
Henvendelsen fra Datatilsynet skete som opfølgning på en sag fra 2008, også med fejlagtig offentliggørelse af personfølsomme oplysninger fra Lokaludvalgenes dagsordener og beslutningsprotokoller. På daværende tidspunkt blev de omtalte oplysninger straks fjernet, og alle lokaludvalgssekretærer instrueret i hvordan tilsvarende sager skulle undgås i fremtiden.
Da Center for Borgerservice ikke umiddelbart kunne danne sig et overblik over problemets omfang, og da det ikke kunne udelukkes, at der lå andre hjemmesider med adgang til lignende oplysninger, besluttede Center for Borgerservice at lukke for adgangen til lokaludvalgenes dagsordener og beslutningsprotokoller. Samtidig blev de links, CBS havde modtaget fra Datatilsynet gjort inaktive.
Efter aftale med BR-sekretariatet gennemgik samtlige lokaludvalg deres dagsordener, beslutningsprotokoller samt materiale, som lokaludvalgene havde lagt ud på hjemmesiderne via Sitecore for fortrolige og personfølsomme oplysninger, med henblik på at få fjernet oplysningerne fra de servere, som kommunen anvender, samt kontakte relevante søgemaskiner med henblik på at få fjernet evt. materiale fra disse søgemaskiners cache mv.
Konsekvenser i forlængelse af hændelsen.
Der blev i forbindelse med hændelsen ikke iværksat foranstaltninger over for personalet.

Hvilke foranstaltninger er gennemført.
Der er efterfølgende blevet afholdt et internt kursus, hvor BR-sekretariatet har undervist lokaludvalgenes medarbejdere i sikkerhedsreglerne i persondataloven og offentlighedsloven m.v. Derudover er der udsendt en vejledning til samtlige sekretariater med en række rutiner, der skal følges i forbindelse med publicering og anden offentliggørelse på nettet. Endelig er hvert

lokaludvalgssekretariat blive bedt om at udpege en person, der er ansvarlig for at der ikke i fremtiden kan findes personfølsomme og fortrolige oplysninger på Internettet.

Bilag 2

It-sikkerhedsbrud i Økonomiforvaltningen 2009 - Koncernservice

Hændelsen
I forbindelse idriftsættelse af nyt Flexvalgssystem (bruttolønsystem) blev det konstateret at systemet ikke levede op til kravene om håndtering af passwords jf. it-sikkerhedsregulativets § 55, samt it-sikkerhedsregulativets § 60, som omfatter medarbejderens ansvar, for at password er personligt og fortroligt.
Overtrædelsen bestod i at systemets register for Password ikke var krypteret og det derfor var muligt for 2 medarbejdere med særlige rettigheder, at slå op i systemet og se hvilke password en medarbejder havde angivet ved pålogning af systemet. Dette med henblik på at kunne videregive dette til medarbejdere som havde glemt deres Password.

Konsekvenser i forlængelse af hændelsen.
Som følge af at Systemet var idriftsat med henblik på medarbejderes bestilling af Transportkort hos Movia var det ikke muligt at lukke adgangen til systemet, idet dette ville betyde en udskydelse af bestillingsproceduren for medarbejderes adgang til at bestille transportkort.
Det blev på denne baggrund aftalt at dispensere for reglerne i IT sikkerhedsregulativet således at medarbejderes tilmelding til transportkortordningen kunne afsluttes.
Der blev i denne forbindelse indskærpet over for de 2 medarbejdere, som var givet adgang til systemets passwordregister at, adgangen skulle foregå under skærpet sikkerhed.
Ved tilmeldingsperiodens udløb blev de pågældende medarbejderes adgang til systemet lukket.

Hvilke foranstaltninger er gennemført.
Iflg. it sikkerhedsregulativets § 69. er det ved anskaffelse og udvikling af it-systemer, systemejer som skal sikre, at anskaffelsen og udviklingen lever op til de gældende it-sikkerhedskrav og kommunens it-strategi.
På baggrund af sagen er det indskærpet over for systemejer, samt dennes daglige leder, at der i forbindelse med kommende udbud skal være indarbejdet krav om passwordsikkerhed, samt at der skal være skærpet fokus på overholdelse af IT sikkerhedsregulativets krav til systemanskaffelse samt opbygning af systemets sikkerhedsdel.

Bilag 3

It-sikkerhedsbrud i Kultur- og Fritidsforvaltningen 2009

1. Marts 2009 – udlevering af brugerident
   - En ekstern konsulent har fået udleveret langtidssygemeldt medarbejders brugerident i forbindelse med mindre udviklingsopgave.
   - Sikkerhedsbruddet kan henføres til it-sikkerhedsregulativets § 54 stk. 1, hhv. § 60 stk.1, omhandlende personlige brugeridenter.

   Løsning:
   - De personalemæssige konsekvenser er håndteret med en mundtlig indskærpelse af sikkerhedsbestemmelserne over for medarbejderen.
   - Der er iværksat generelle awareness-aktiviteter i KFF omkring it-sikkerhed, både i form af månedlige sikkerhedstip og initiering af struktureret information for nye medarbejdere.

2. Marts 2009 – installation af ikke-godkendt software
   - En leder har erfaret ikke-autoriseret software installeret på en arbejds-pc. Programmerne er ikke 'ondsindede', og der er ikke konstateret uregelmæssigheder i øvrigt.
   - Det har ikke været muligt at påvise, hvornår det er foregået, eller hvem der har udført dette, men forskellige ting peger på, at det er udført af en konkret medarbejder.
   - Sikkerhedsbruddet kan henføres til it-sikkerhedsregulativets § 65 stk.3, omhandlende indstillinger på arbejdsstationer, hhv. § 70 stk. 3-4, omhandlende autoriserede programmer og ophavsret.

   Løsning:
   - Medarbejderen er, trods benægtelsen af kendskab til hændelsen, mundtligt blevet indskærpet sikkerhedsbestemmelserne, og har tillige fået besked om, at gentagende tilfælde kan få ansættelsesretlige følger.
   - Der vil opfølgningsmæssigt blive gennemført kontrol af installeret software og rettigheder på den pågældende arbejds-pc.

3. September 2009 – anvendelse af fælles brugeridenter
   - I forbindelse med support og fejlretning er der observeret anvendelse af fælles brugeridenter.

- Konsekvensen er, at det ikke i alle sammenhænge er muligt at henføre systemmæssige aktiviteter og handlinger til en specifik medarbejder. Anvendelsen af disse fælles brugeridenter, som hænger sammen med visse historiske og forretningsmæssige hensyn, er ikke et nyt fænomen, men har ikke tidligere været formelt synliggjort.
- Sikkerhedsbruddet kan henføres til it-sikkerhedsregulativets § 54, omhandlende personlige brugeridenter, hhv. § 60 stk. 1 og 3, omhandlende personlige og fortrolige adgangskode samt flere brugeres anvendelse af samme arbejdsstation.

Løsning:

- Dokumentation af den konkrete anvendelse af fælles brugeridenter er under udarbejdelse. Denne vil beskrive i hvilke sammenhænge, og hvilke systemer, der indgår i anvendelsen, således at forretningens behov kan bruges som input til kravspecifikation omkring fremtidige løsninger.
- I fald der ikke findes løsninger, eller disse anses for forretningsmæssigt uhensigtsmæssige, vil forvaltningen søge dispensation efter gældende retningslinier.

Bilag 4

It-sikkerhedsbrud i Børne- og Ungdomsforvaltningen 2009

(Beskrivelsen er *anonymiseret af BUF's sekretariat*)

To brugeradministratorer i BUF's sikkerhedsadministration har i perioden maj 2008 til marts 2009 benyttet samme brugerId til at oprette brugere i RACF/ZI. Samme fremgangsmåde er anvendt i perioden april 2009 til september 2009.
BUF's brugeradministration blev frem til februar 2008 udført af de stedfortrædende sikkerhedsledere. På grund af et stigende antal autorisationer og ændringer blev yderligere en medarbejder ansat som brugeradministrator 1. marts 2008. Efter en kort oplæring skulle denne fra maj 2008 selvstændigt oprette brugere og tildele dem rettigheder også i RACF/ZI-systemet. På denne baggrund anmodede BUF BR's sekretariat om at få mulighed for at benytte endnu en sikkerhedsadministrator. Dette blev afvist med henvisning til, at det ikke var teknisk muligt i ZI-systemet. Man havde godt nok bestilt en ændring med henblik på at anvende flere brugeradministratorer i KS, men man ville ikke udvide denne mulighed til BUF på grund af omkostningerne og den begrænsede tid, man havde brug for en sådan ændring.
Ved en beklagelig fejl var brugeradministrationen ikke opmærksomme på, at dette betød, at der kun kunne være to medarbejdere, som kunne gennemføre brugeradministration i ZI-systemet, og man indledte en praksis, hvor både to medarbejdere benyttede samme konto til brugeradministration. BR's sekretariat blev opmærksomme på denne praksis i marts 2009 og forlangte, at den blev bragt til ophør. Dette skete 6. april 2009.
I forbindelse med ophøret af den uretsmæssige praksis foreslog Center for Informatik, at man etablerede en udvidelse af kontoen ved at fastlåse den til de to brugeradministratorers terminalId, samtidig med at deres terminalId blev bundet til deres fysiske PC'er. Denne løsning blev forhåndsgodkendt af den interne it-revision, men blev ikke umiddelbart iværksat, da man besluttede, at en af brugeradministratorerne i stedet skulle "låne" en brugeradministrator-Id af Koncernservice. Denne blev aldrig stillet til rådighed og den uretmæssige brug blev genoptaget frem til september 2009, hvor den blev indstillet.
BUF beklager det skete og har ved gennemgang af de daglige sikkerhedsrapporter ikke konstateret misbrug af den uretmæssige fremgangsmåde.

Bilag 5

It-sikkerhedsbrud i Teknik- og Miljøforvaltningen 2009

Der er konstateret 4 hændelser i Teknik- og Miljøforvaltningen, som ifølge kommunens it-sikkerhedsregulativ karakteriseres som it-sikkerhedsbrud.
Det drejer sig om følgende typer af hændelser:

- I 3 tilfælde har medarbejdere udlånt password til en eller flere kolleger.
- I ét tilfælde har konsulent, ansat af TMF, haft lemfældig omgang med egne og andres brugerid og password, i form af påsatte post-it sedler med de omtalte informationer.

Sikkerhedsbruddene har ikke medført nogen konsekvenser i forhold til økonomi, revision, politi eller lignende.
Det er indskærpet overfor medarbejdere og ledelse, at reglerne på it-sikkerhedsområdet skal overholdes, lige som direktionen er orienteret om hændelserne, konsekvens og iværksatte foranstaltninger.
De omtalte sikkerhedshændelser kan karakteriseres som skødesløshed og manglende omtanke fra medarbejdere/konsulent side.
For at imødegå lignende hændelser i fremtiden, har der i løbet af året været generelle awareness-aktiviteter i forvaltningen, i form af "Info" på Teknik- og Miljøforvaltningens KKnet forside. Informationen vedrører især emnet omkring de personlige brugeridenter og password fortrolighed.
Sidst på året forventes en it-sikkerhedsportal implementeret på forvaltningernes intranet KKnet. Portalen er et nyt fælleskommunalt værktøj, som vil kunne understøtte medarbejdernes viden om it-sikkerhed.

Bilag 6

It-sikkerhedshændelser i Socialforvaltningen 2009

(Beskrivelsen er *anonymiseret af SOF's sekretariat*)

Foranlediget af indberetning om; at der blev anvendt fælles brugeridenter har It-sikkerhedsleder i SOF foretaget et kontrolbesøg på en institution.

På et møde samtykkede institutionens leder i, at det havde været fast praksis gennem flere år at anvende fælles brugeridenter.

Lederen fremførte, som argument herfor bl.a. "at det gennem flere år havde været vanskeligt at få oprettet brugere. Endvidere var der døgnåbent og det tog lang tid at logge ind og ud."

Disse argumenter retfærdiggør dog ikke en overtrædelse af reglerne.

It-sikkerhedslederen orienterede derfor om, at denne praksis skulle stoppe øjeblikkelig. Hver bruger skulle have sin egen brugerident og password, som ingen andre måtte bruge. Jævnfør Persondatalovens § 41 og Regulativ for it-sikkerhed i Københavns Kommune af 15. maj 2008 § 60 stk. 1. "Adgangskoder må ikke udlånes til andre. De er personlige og strengt fortrolige" samt 52 stk.1 "al adgang til kommunens it-systemer, (..) skal være betinget af konkrete autorisationer."

Baggrunden for dette er, at man i misbrugstilfælde entydigt skal kunne fastslå hvem der er ansvarlig. Ved hjælp af den personlige brugerident kan man i "loggen" se hvem der har misbrugt systemet og til hvad.

Der er endvidere til orientering i december 2008 indført en væsentligt enklere og hurtigere måde at oprette brugeridenter på, idet SOF er overgået til rollebaserede brugerprofiler.

På mødet oplyste institutionslederen, at alle medarbejdere nu var orienteret om at skifte password.

It-sikkerhedslederen gav frist i 20 dage til at bringe tingene i orden og få oprettet de nødvendige nye brugere.

Ved efterfølgende kontrol blev det konstateret, at forholdet nu er bragt i orden: Passwords er ændret. Fælles brugeridenter er taget ud af brug. Der er efter mødet blevet oprettet et antal nye individuelle brugeridenter og andre er blevet ændret.

Kontorchefen for Fagkontoret har givet institutionslederen en mundtlig påtale.

Sagen betragtes hermed som afsluttet.