KØBENHAVNS KOMMUNE
Økonomiforvaltningen
Koncernservice

NOTAT

23-04-2015

Bilag til punkt 9 "Styrkelse af it-sikkerheden" på Borgerrepræsentationens møde 30. april 2015

Sagsnr.
2014-0205519

Dokumentnr.
2014-0205519-12

Sagsbehandler
Mette Høgholt Lønne

Sagsbeskrivelse
Økonomiudvalget har på møde 14. april 2015 anbefalet indstilling om investeringer til styrkelse af it-sikkerheden i Københavns Kommune.

Nærværende notat indeholder (1) en overordnet tidsplan for implementering af aktiviteterne samt (2) en beskrivelse af de seneste tre års sikkerhedsbrud.

1. Tidsplan for implementering af aktiviteterne
Koncernservice vil sikre at aktiviteterne igangsættes umiddelbart efter frigivelse af bevillingen i Borgerrepræsentationen.

Implementeringsprojektet afsluttes i 2015, og opfølgende aktiviteter håndteres i drift af løsningerne i 2016 og frem.

Den planlagte tidsplan for implementering af aktiviteterne er beskrevet i nedenstående tabel:

Aktivitet	Beskrivelse	Start	Deadline
Styring af informationssikkerhed gennem anskaffelse og drift af en log- og event management-løsning (SIEM)	Systemet implementeres og centrale fælles systemer i KS overvåges	4. maj 2015	Ultimo december 2015
	Udbygning af løsning med fag-applikationer fra forvaltningerne sker i en kontinuerlig proces som led i driften af løsningen fra 2016, således at systemer løbende inddrages i overvågningen		
Etablering af ny struktur på datanetværket	Ændring gennemført	4. maj 2015	Ultimo december 2015

Ledelsessekretariatet

Borups Allé 177
2400 København NV

Telefon
2169 3046

EAN nummer
5798009809056

Styring af lokale administrations-rettigheder	Overdragelse til fuld drift	4. maj 2015	Ultimo august 2015
Ekstern overvågning af hændelser på netværket	Overdragelse til fuld drift	4. maj 2015	Ultimo august 2015
Webscanner	Overdragelse til fuld drift for kk.dk	4. maj 2015	Primo september 2015
	Fortsat udbygning af løsning med nye KK drevne sites - kontinuerlig proces som led i drift af løsning		
Foranalyse og etablering af business case vedr. automatisering af adgangsstyring.	Foranalyse med opstilling af business case gennemført	4. maj 2015	Ultimo november 2015
	Indstilling til ØU		Primo januar 2016

Koncernservice vil afrapportere fremdrift i projektet hver 3. måned, startende ultimo august 2015.

2. Beskrivelse af de seneste tre års sikkerhedsbrud

Aktuelle hændelser og trusler mod It-sikkerheden
Koncernservice har i dag ikke fuldt overblik over de faktiske hændelser på It-sikkerhedsområdet i Københavns Kommune, idet Koncernservice (It-sikkerhedsfunktionen) kun medvirker i udredning af konkrete hændelser efter anmodning fra forvaltningerne, og dermed er afhængig af hændelserne indberettes.

Med de foreslåede investeringer vil Koncernservice få et samlet overblik over aktiviteterne på både de centrale fælles systemer og centrale fagsystemer i forvaltningerne. Det vil give et langt bedre overblik end i dag og vil muliggøre at der bliver etableret et samlet "normalbillede" over aktiviteter på systemerne. Det giver mulighed for at identificere og imødegå sikkerhedshændelser før de udvikler sig til sikkerhedsbrud.

Koncernservice har registreret over 80 It-sikkerhedshændelser af meget varierende karakter siden 2013. De er nærmere beskrevet nedenfor.

Personalesager om misbrug af rettigheder
Koncernservice har aktuelt kendskab til at der i 2014 har været 7 tjenstlige personalesager vedr. It-sikkerhedshændelser, typisk på baggrund af misbrug af rettigheder.

Fejlagtig offentliggørelse af følsomme og fortrolige personoplysninger
Koncernservice har kendskab til 2 konkrete sager vedr. fejlagtig offentliggørelse af følsomme og fortrolige personoplysninger på kommunens hjemmesider.

- Datatilsynet har henvendt sig på baggrund af fejlagtig offentliggørelse af CPR oplysninger om borgere på kommunens hjemmeside. Det drejede sig om et dokument fra dagsordenssystemet som indeholdt følsomme personoplysninger om 13 borgere. Oplysningerne blev straks fjernet og de berørte borgere blev informeret om fejlen.
- En borger informerede Koncernservice om at der lå følsomme personoplysninger gemt i en PowerPoint fil publiceret af et sundhedsteam på en kommunal hjemmeside. Data blev straks fjernet.

Andre typer hændelser
Andre typer hændelser er f.eks.: Fejlagtig tildeling af rettigheder, uautoriseret software, ikke godkendt udstyr tilsluttet kommunens administrative net, misbrug af login og tyveri af udstyr.

De registrerede hændelser udgør imidlertid kun ”toppen af isbjerget”.

Kommunens netværk har været udsat for flere målrettede og koordinerede DDos angreb der typisk blokerer kommunens netværkstrafik. Den type angreb har vist sig løbende at tage til i styrke.

Kommunens netværk angribes konstant af eksterne hackere og kriminelle, der ønsker at anvende den kommunale infrastruktur til uvedkommende formål. Overvågning af netværkstrafikken viser således forsøg på at etablere skjulte ”trojanske heste”, der kan anvendes til uvedkommende, typisk kriminelle formål rettet mod andre eksterne organisationer og som potentielt truer drifts- og datasikkerheden i Københavns kommune.

Kommunens spamfilter afviser dagligt mere end 1.900.000 uvedkommende mails.

Der bliver typisk afvist over 6000 forskellige vira hver måned.

Ransomware - angreb
En særlig type it-angreb kaldet ransomware florerer og har 2 gange direkte ramt kommunen her i 2015.

Det er avancerede angreb hvor medarbejdere via en umiddelbart troværdig mail er blevet narret til at klikke på et link, der straks installerer ondsindet kode på pc´en, Når det sker, bliver alle drev med filer som medarbejderen har adgang til krypteret. Det betyder typisk, at al adgang til filer i en hel enhed er spærret. Det er hver gang lykkedes Koncernservice at reetablere data, men det har hver gang krævet et stort oprydningsarbejde for både Koncernservice og den involverede forvaltning.

Awareness tiltag.
En af kommunens største trusler mod It-sikkerheden er medarbejderne selv. Medarbejderne skal vide, hvilke retningslinjer de skal følge, da korrekt adfærd er en væsentlig forudsætning for at sikre kommunen mod angreb.

Koncernservice It-sikkerhed udarbejder derfor løbende awareness materiale, der publiceres på intranettet tilgængeligt for alle forvaltninger. Det er fx artikler til KKintra eller vejledninger til It-sikkerhedshåndbogen.

I 2014 udarbejdede Koncernservice en fuld awareness-kampagnepakke til alle forvaltninger med video, pjecer, artikler m.v. Pakken indeholdt materiale og plan der ville gøre forvaltningerne i stand til selv at gennemføre kampagnen lokalt. Kampagnepakken blev sendt ud til ledelsen i alle forvaltninger, med tilbud om hjælp til planlægning af den lokale kampagne.

Koncernservice tilbyder fortsat hjælp til implementering af det udsendte kampagnemateriale eller gennemførelse af andre awareness-initiativer efter de enkelte forvaltningers behov.