KØBENHAVNS KOMMUNE
Økonomiforvaltningen
Koncernservice

NOTAT

07-04-2017

Sagsnr.
2017-0008394

Dokumentnr.
2017-0008394-2

Sagsbehandler
Kirsten Wenning

Til Økonomiudvalget

Aflæggerbordet

Orientering til Økonomiudvalget om status på it-sikkerhedsarbejdet og it-sikkerhedshændelser i 2016

Baggrund

I henhold til kommunes it-sikkerhedsregulativ orienterer it-sikkerhedsfunktionen i Koncern IT mindst en gang årligt Økonomiudvalget om status på it-sikkerhedsarbejdet i kommunen, og herunder om it-sikkerhedshændelser og kompenserende tiltag.

It-sikkerhedsarbejdet

Københavns kommune har i løbet af 2016 arbejdet målrettet med styrkelse af it-sikkerheden på flere områder.

Brugerstyring

Borgerrepræsentationen har på forslag fra Økonomiforvaltningen besluttet, at it-sikkerhedsarbejdet skal styrkes væsentligt på flere centrale områder: Det er et arbejde, der pågår og intensiveres i 2017 og frem. Det drejer sig om:

1. Anskaffelse af en Identity Management (IDM/IGA) løsning til automatisering af brugerstyring og omlægning af forretningsgange i forvaltningerne og Koncernservice.
2. Renovering af Københavns Kommunes Active Directory (AD), der er det grundlæggende infrastrukturelement til brugerstyring i Københavns Kommunes samlede it-installation. En renovering er en forudsætning for et velfungerende IDM/IGA system.

Målet er hermed at forbedre it-sikkerheden, imødekomme revisionsanmærkninger og kunne leve op til lovgivningskrav i forbindelse med Databeskyttelsesforordningen.

Risikostyring

Økonomiforvaltningen (Koncern IT) har på basis af en samlet risikostyringsmodel udarbejdet proces og værktøjer til brug for gennemførelse af risikovurderinger af kommunens systemer. En risikostyringsmodel og de tilhørende processer gør det muligt både at vurdere risikoen for de enkelte systemer og etablere et samlet risikobillede for den enkelte forvaltning og for kommunen som helhed. Med budget 2017 er der bevilget ressourcer til, at it-sikkerhedsfunktionen i Koncern IT kan overtage ansvaret for at gennemføre risikostyringsprocessen på it-området for forvaltningerne. Arbejdet med konkrete risikovurderinger i forvaltningerne er påbegyndt 1. kvartal 2017.

It Driftscenter

Borups Allé 177
2400 København NV

Mobil
2673 1102

EAN nummer
5798009809308

SIEM log- og eventmanagement
Styring af informationssikkerhed er forbedret gennem it-sikkerhedsfunktionens drift af log- og event management-løsningen (SIEM). Systemet bruges til opsamling og vurdering af logs fra systemer med følsomme persondata og værdidata og proaktivt i forhold til at opdage og finde årsagen til utilsigtede hændelser, f.eks. hackerangreb eller andre trusler mod driftssikkerheden. Systemet omfatter pt. overvågning af en række centrale fællessystemer i Koncernservice/Koncern IT og er i 2016 løbende udbygget med overvågning af logs fra udvalgte kritiske fagsystemer fra forvaltningerne. På baggrund af rapporter fra SIEM kan forvaltningernes systemejere reagere på utilsigtede hændelser. Arbejdet med udbygning af overvågning af kritiske systemer videreføres i 2017.

It-anskaffelsesprocessen
Forud for idriftsættelse af it-systemer i kommunen skal systemerne gennemløbe en it-anskaffelsesproces. Her har it-sikkerhedsfunktionen ansvar for, at der foretages it-sikkerhedsvurdering af de samlede it-sikkerhedsmæssige forhold omkring systemet, og herunder om persondatalovgivningen overholdes og om systemet lever op til kommunens it-sikkerhedsregler. It-sikkerhedsvurderingen sker med henblik på, at systemet afslutningsvis kan modtage en ibrugtagningstilladelse. For at tydeliggøre ansvar og opgaver i forbindelse med it-anskaffelsesprocessen, er der i samarbejde med forvaltningerne udarbejdet en samlet proces og beskrivelse af it-sikkerhedsfunktionens arbejde med it-sikkerhedsvurderinger. It-sikkerhedsfunktionen foretager gennemsnitlig 28 it-sikkerhedsvurderinger om måneden.

Sikring af datanetværket
Efter en større indsats i 2016 er etablering af ny struktur på datanetværket tæt på en afslutning. Omlægningen skal sikre, at det kun er autoriseret udstyr, der kan tilsluttes det administrative netværk. Ved udgangen af 1. kvartal 2017 vil 98 % af kommunens net være omlagt, de resterende 2 % afventer etablering af ny telefoniplatform sommeren 2017.

Webscan for CPR-numre
Drift af Webscanner er løbende udbygget. Således er både www.kk.dk og øvrige KK drevne sites medtaget i den overvågning og scanning, der gennemføres af kommunens interne og eksterne hjemmesider for at forhindre fejlagtig offentliggørelse af CPR-numre.
Koncern IT har via scanning af kommunens hjemmesider identificeret flere tilfælde, hvor medarbejdere utilsigtet har offentliggjort dokumenter indeholdende CPR- numre på kommunale sites på internettet. Koncern IT håndterer observationen ved at kontakte de

ansvarlige for sitet med besked om straks at fjerne de fortrolige oplysninger fra internettet, evt. borgerunderretning og besked om at indskærpe forbedring af procedurer for publicering, for at undgå lignende situation i fremtiden.

Sundhedscheck
Koncern IT har i 2016 gennemført "sundhedscheck" af 16 systemer særligt inden for økonomi, med henblik på sikring af driftsstabilitet og tilstrækkelig dokumentation af kritiske systemer. 9 systemer levede op til kravene i "sundhedscheck" mens der var mangler i dokumentationen for de resterende systemer. Koncern IT har anmodet de ansvarlige om at udbedre dokumentationen, og Koncern IT vil følge op på sagen igen i 2017 som led i gennemførelse af risikostyringsprocessen i forvaltningerne.

Awareness.
Københavns kommunes datasikkerhed og eksponering for cyberkriminalitet er i høj grad afhængig af medarbejdernes adfærd. Det er derfor nødvendigt, at uddanne og informere medarbejderne om aktuelle trusler og kommunens retningslinjer på kritiske områder. Derved kan risikoen for kompromittering af kommunens it-systemer og tab af fortrolige informationer minimeres.
Koncern IT udarbejder løbende awareness-materiale og kampagner med henblik på at højne bevidstheden om it-sikkerhed i kommunen. I 2016 er der gennemført awareness-kampagner på væsentlige områder som:

- It-sikkerhed og persondata på mobile enheder
- Truslen fra It-kriminelle, ransomware og phishing

Som led i kampagnerne har Koncern IT oprettet et kampagnesite på kommunens intranet med relevant informationsmateriale fx pjecer og film.
Kampagner og materiale retter sig mod forvaltningerne og deres medarbejdere.

It-sikkerhedshændelser og trusler mod it-sikkerheden
Koncern IT har i 2016 registreret og håndteret en række væsentlige hændelser på it-sikkerhedsområdet i Københavns Kommune.

Cybercrime
Ransomware har ramt kommunen 5 gange i 2016. Angrebstypen er meget avanceret og narrer medarbejdere til at åbne og klikke på inficerede filer og links. Når kommunen rammes, betyder det ofte, at mange filer på netværksdrev bliver krypteret, låst og dermed utilgængelige for medarbejderne i længere tid. Koncern IT hjælper forvaltningerne med at løse problemet ved at genindlæse filer fra backup.

Overbelastningsangreb, - også kaldet DDos angreb, har været i kraftig vækst i 2016 og har ramt kommunen over 100 gange. Det er målrettede og koordinerede angreb, der typisk blokerer kommunens netværkstrafik. Angrebene har været mere eller mindre omfattende. Nogle har været målrettet www.kk.dk, andre subsites til kommunens hjemmeside og igen andre kommunens VPN forbindelser (Virtuel Private Network). Koncern IT har håndteret disse angreb i samarbejde med ekstern leverandør, og der er fra 2017 indgået aftale om automatiseret overvågning til at opnå forbedret beskyttelse mod angrebene.

Svindlere har med Social Engineering forsøgt at målrette falske e-mails mod økonomimedarbejdere fra kommunes forvaltninger. Med falske e-mails er f.eks. anmodet om oprettelse af pengeoverførsler til udenlandske banker, idet mailene så ud til at være sendt fra medarbejdere og chefer med bemyndigelse til at godkende sådanne transaktioner**.** Koncern IT har i videst muligt omfang blokeret for de falske e-mails og tilhørende hjemmesider, samtidig med at kommunens medarbejdere er blevet advaret.

Øvrige hændelser og kompenserende tiltag
Koncern IT har i 2016 fundet skadelig kode på en server overført fra eksternt datacenter. Serveren driftsafviklede en offentlig hjemmeside for en enhed i Københavns Kommune, den skadelige software åbnede op for, at eksterne havde muligt for at overtage serveren og derved få adgang til data, og bruge den som platform for angreb på andre interne og eksterne servere. Koncern IT lukkede straks umiddelbart efter ned for ekstern adgang til serveren, og i samarbejde med forvaltningen blev der etableret en ny serverløsning med en ny, tidssvarende hjemmeside med tilstrækkelig sikkerhed for forvaltningen. Koncern IT vurderede efter en nærmere analyse, at den skadelige software ikke var anvendt i den tid, serveren har været opsat i Københavns Kommunes it-miljø.

Øvrige registrerede hændelsestyper er f.eks. fejl i rettigheder, softwarefejl, misbrug af login, usikker opbevaring af dokumenter med fortrolige oplysninger og tyveri af bærbare computere. I alle tilfælde har it-sikkerhedsfunktionen fulgt op på hændelser i samarbejde med de involverede ledere og medarbejdere og i nødvendigt omfang revideret gældende vejledninger og instrukser.

En stor del af de it-angreb, Københavns Kommune bliver udsat for, kommer via reklamebannere. Derfor blev der fra januar 2016 blokeret for adgang fra det administrative netværk til reklamebannere på internettet.

Kommunens antispam-/virusfilter afviser over 5.000.000 uvedkommende mails om måneden, heraf indeholder mindst 1200 mails decideret ondsindede vira.