HVIDBOG

HVIDBOG OM GOD KOMMUNAL SIKKERHEDS-KULTUR

Hvidbog om god kommunal sikkerhedskultur

1. udgave, 1. oplag 2019

Produktion: Kommuneforlaget A/S
Design: e-Types
Tryk: KL's Trykkeri
Foto: Fremfærd Borger

KL
Weidekampsgade 10
2300 København S
Tlf. 3370 3370
kl@kl.dk
www.kl.dk
@kommunerne
facebook.com/kommunerne

Produktionsnr. 830510
ISBN 978-87-93668-80-5
ISBN 978-87-93668-81-2-pdf

HVORFOR ER SIKKERHEDSKULTUR VIGTIGT?

Øget digitalisering fordrer stærke sikkerhedskompetencer i organisationen og kan kun ske, såfremt borgerne fortsat bevarer den digitale tillid. Det kan sikres gennem anvendelse af en solid it-hygiejne, der hjælper kommunen med at løse nogle af de sikkerhedsmæssige problemer; brugere kan underlægges systematiske regler for kodeord og brugeradgang, og data kan krypteres og slettes automatisk efter en periode.

Teknologi løser dog ikke alle problemer. Der er ganske enkelt for mange regler og for stor kompleksitet i emnet datasikkerhed, til at kommunale medarbejdere kan have et indgående kendskab til alle regler og procedurer og de hurtigt skiftende trusler fra it-kriminelle.

I stedet bør der arbejdes efter, at medarbejdere har tilstrækkelige kompetencer til at kunne vurdere de enkelte dilemmaer og handle ud fra organisationens sikkerhedskultur, når der opstår sikkerhedsmæssige problemer.

Datasikkerhed kan ikke ses som en separat faglighed, der hører til i it-afdelingen, men som en naturlig del af hele organisationens kernekompetencer. De kommunale medarbejdere behøver ikke at kunne løse alle sikkerhedsmæssige dilemmaer selv, men skal have de fornødne kompetencer til at kunne identificere de sikkerhedsmæssige problemstillinger, når de opstår i betjeningen af borgere. Herudover skal de kunne forholde sig kritisk til hvorvidt de selv kan løse problemet, eller om de skal søge hjælp i organisationen.

DIGITAL AWARENESS

Den digitale udvikling stiller krav til at medarbejdere og ledere udviser en høj grad af awareness i omgangen med borgernes data. Men begrebet er diffust, for hvad det vil sige at være aware? Awareness er et begreb, som ikke er almindeligt brugt i Danmark, men det engelske aware kan oversættes til det at være bevidst – både i tanke og handling.

At medarbejdere og ledere besidder digital awareness betyder, at de er bevidste om, hvordan de behandler borgernes data - ikke bare i forhold til, om de it-systemer, de bruger, nu også er sikret mod f.eks. hacker-angreb - men også, at man i den daglige omgang med data ved, hvad man må og ikke må. At man ved hvordan man agerer i situationer, hvor borgerne f.eks. beder om noget, som kan udsætte dem selv for risiko for læk, eller udefrakommende misbrug af deres data.

Historier om datalæk eller uheld med data i kommunerne peger nogle gange tilbage på medarbejdere, der får trykket på en forkert knap eller får sendt data i en mail, man ikke skulle have sendt.

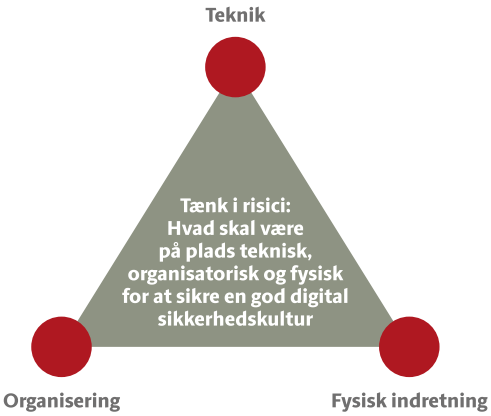
Men man skal passe på ikke at individualisere ansvaret for sikkerhed, så det er den enkelte medarbejder, der står med ansvaret alene.

I stedet skal der arbejdes med sikkerhed som en kultur i forhold til hele organisationen, så den høje tillid og tryghed, som danskerne har til kommunerne, kan fastholdes.

RISIKOTREKANT

God kultur for informationssikkerhed hviler på tre dimensioner: Den tekniske, den fysiske indretning og organiseringen omkring informationssikkerhed. Treenigheden danner en risikotrekant, og har man fokus på alle tre sider i trekanten, så kommer man godt rundt om mange af de problemstillinger, som kommunerne kommer ud for, når det gælder informationssikkerhed og kontakt med borgerne.

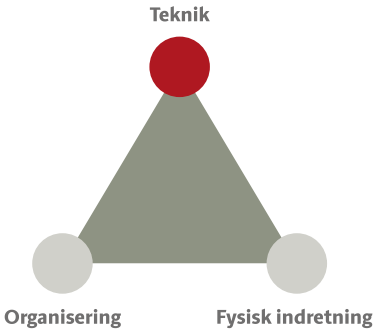
› Figur: Risikotrekant



TEKNIK

Den første side af trekanten vedrører teknik.

› **Figur: Teknik**



Se otte tips om det tekniske aspekt – god systemadfærd.

Tip nr. 1 Hav et tydeligt lederfokus på, hvad god systemadfærd er, og lad lederne gå forrest. De er rollemodeller for resten af afdelingen.

Tip nr. 2 Er jeres informationssikkerhedspolitik klar? Lad den have et tydeligt fokus på, hvordan man behandler og passer på borgernes data på både computere og andre digitale enheder, som enten står fast på arbejdspladsen, eller som kan tages med ud af huset.

Tip nr. 3 Sørg for, at der er fastlagt regelmæssige lederkontroller, der sikrer, at medarbejdere og ledere har de korrekte systemadgange og brugerprofiler.

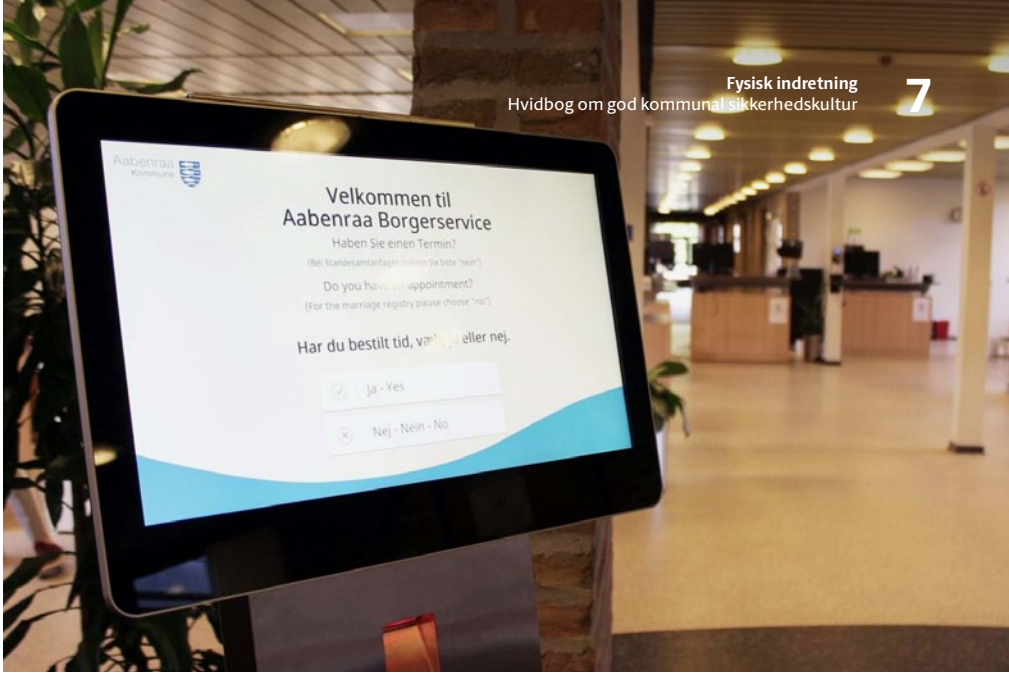
Tip nr. 4 Sørg for jævnlige stikprøver, der kontrollerer, hvilke systemer medarbejderne bruger, når de løser bestemte opgaver.

Tip nr. 5 Sørg for klare instrukser for, hvordan bestemte opgaver håndteres. Når der skal oprettes en ny medarbejder i bestemte IT- og fagsystemer, ligger der så en klar godkendelse fra en leder? Hvordan er instrukserne for medarbejdernes adgange, når de fratræder igen eller skifter afdeling?

Tip nr. 6 Brug sikker mail hver gang, I kommunikerer med borgere digitalt.

Tip nr. 7 Sørg for, at der dokumenteres korrekt, og at dokumentationen gemmes direkte i fagsystemerne.

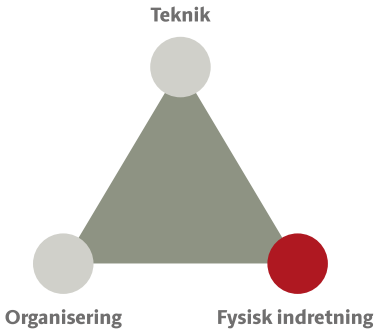
Tip nr. 8 Sørg for, at det er fastlagt, hvem der godkender, når der skal indkøbes eller tages nye IT-systemer i brug. Har I en visitationsgruppe, et digitaliseringsråd eller lignende, der sikrer, at systemerne er tilpasset den fælles it-arkitektur?



FYSISK INDRETNING

Den anden side af trekanten handler om fysisk indretning.

› Figur: Fysisk indretning



En hensigtsmæssig indretning af lokaler kan være med til at styrke sikkerheden og beskytte borgeren, borgerens data og medarbejderne.

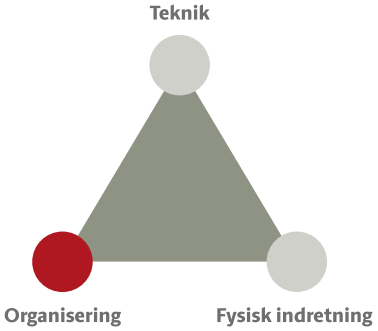
Her tænkes på de områder, hvor der sker møde med borgeren. Er det muligt at gå ind i et lokale, hvis en forælder ønsker en samtale med en lærer? Er borgerservicelokalet indrettet hensigtsmæssigt, så borgernes oplysninger kan beskyttes?

Tips til fysisk indretning af borgerservice kan findes via nedenstående link.
vpt.dk/aware/indretning

ORGANISERING

Den tredje side af trekanten handler om organisering.

› Figur: Organisering



Her følger fem konkrete tips til, hvordan man kan arbejde med det organisatoriske aspekt af informationssikkerhed.

Tip nr. 1 Har I en fast struktur for, hvordan I deler viden med hinanden? F.eks på afdelingsmøder eller teammøder. At sætte informationssikkerhed på dagsordenen som et fast punkt, hver gang I holder møder, kan gøre, at bevidstheden om informationssikkerhed bliver højere hos alle. Gennemgå f.eks. konkrete arbejdsgange eller vejledninger, så alle har et fælles billede. Lav referater fra møderne, og sørg for, at det er obligatorisk og godkendt af ledelsen, at medarbejderne bruger tid på at læse mødereferaterne.

Tip nr. 2 Opret og brug en hændelseslog, hvor I kort beskriver, når der er sket en hændelse, og hvordan I har håndteret den. Med sådan en log får I et værktøj, som I aktivt kan bruge til at dele viden med hinanden i hverdagen.

Tip nr. 3 Når nye medarbejdere starter, så lad dem deltage i et obligatorisk informationssikkerhedskursus, der har fokus på, hvordan man behandler følsomme personoplysninger, bruger sikker mail, dokumenterer i fagsystemer mv. Kurset kan foregå virtuelt eller fysisk, deltagelse bliver noteret, og medarbejderens nærmeste leder bliver orienteret, når kurset er taget, eller hvis medarbejderen ikke har deltaget.

Tip nr. 4 Få udarbejdet målrettet kommunikation om informationssikkerhed til forskellige målgrupper. Vær opmærksom på, at medarbejdere har forskellige læringsstile, så der både er noget til dem, der bedst lærer ved at se, høre eller læse. Brug gerne forskellige virkemidler i kommunikationen. Det kan f.eks. være en kampagne, e-læring, en konkurrence, et motto eller et logo.

Tip nr. 5 Gør en uge hvert år til informationssikkerhedsuge, hvor I sætter særligt fokus på en eller flere problemstillinger inden for informationssikkerhed. Har I f.eks. problemer med falske mails, som forsøger at lokke medarbejderne til at klikke på links, der fører til, at de kan risikere at downloade virus, så planlæg en kampagne på tider af året, hvor det i særlig grad er et problem.

HER ER INFORMATIONS-SIKKERHED EN DEL AF KULTUREN

Brøndby Kommune
I Brøndby Kommune er informationssikkerhed en selvfølgelighed. Den er forankret overalt i organisationen fra direktion til borgerservicemedarbejder og ud i hver enkelt forvaltning.

Brøndby Kommune har 4 råd til at gøre informationssikkerhed til en del af kulturen:

- Lad informationssikkerhed være forankret i direktionen. Træk det ud af IT-afdelingen og gør det til noget, der diskuteres også på direktionsgangene.
- Opret et forum for informationssikkerhedskoordinatorer fra hver sin forvaltning. Her kan der koordineres praktiske ting, udarbejdes politikker, vejledninger, vurderinger mv. Men det er også et forum for forankring af en sikkerhedsfaglighed.
- Prioriter ressourcerne. Send medarbejdere på kursus i sikkerhed og hav en rolle, der går på tværs i organisationen.
- Gå efter motivationen. Informationssikkerhed lyder måske kedeligt, men forsøg at finde det, der motiverer medarbejdere til at arbejde med det. At arbejde systematisk med informationssikkerhed er organisationsudvikling.

Læs mere om hvordan de gør.
vpt.dk/aware/broendby

Aabenraa kommune
I Aabenraa kommune har man udviklet en kultur omkring informationssikkerhed i en travl hverdag.

Her har de arbejdet med fysisk indretning af Borgerservice og tidsbestilling som veje til bedre informationssikkerhed.

Læs mere om hvordan de gør.
vpt.dk/aware/aabenraa

HVILKE KOMPETENCER SKAL DU HAVE FOR AT VÆRE AWARE?

Det er vigtigt, at medarbejdere med direkte borgerkontakt besidder de nødvendige kompetencer til at forstå og efterleve reglerne for beskyttelse af borgerens oplysninger, så borgeren oplever en fortrolig og forsvarlig behandling af sine oplysninger.

Man kan med fordel udnævne informationssikkerhedsambassadører i organisationen, som besidder kompetencer indenfor informationssikkerhed og dermed kan vejlede kolleger i, hvordan borgernes oplysninger beskyttes forsvarligt.

Kompetencehjulet er et værktøj, der kan bruges som udgangspunkt for en diskussion af hvilke kompetencer, der er nødvendige for at arbejde sikkert med information i kommunen.

Værktøjet kan bruge i en MUS-samtale eller på et personalemøde, hvor man ønsker at sætte kompetencer til informationssikkerhed på dagsordenen.

Der er udviklet kompetenceprofiler for funktioner i Borgerservice, IT, specialister og øvrige funktioner.

Læs mere om kompetenceprofilerne på vpt.dk/aware/kompetencer

› **Figur: Kompetencehjul**

En grøn kompetence er en strategisk og/eller personlig kompetence, der understøtter at de faglige kompetencer bedst muligt bringes i spil

En blå kompetence er en faglig kompetence defineret med afsæt i informationssikkerhed

Artikler og materialer, der refereres til i denne hvidbog, er udarbejdet under Fremfærd Borger i et samarbejde mellem KL, BDO, HK Kommunal og 7 kommuner.

Al materiale kan findes på www.erduaware.dk

KL
Weidekampsgade 10
2300 København S
Tlf. 3370 3370
kl@kl.dk
www.kl.dk
@kommunerne
facebook.com/kommunerne

Produktionsnr. 830510
ISBN 978-87-93668-80-5
ISBN 978-87-93668-81-2-pdf