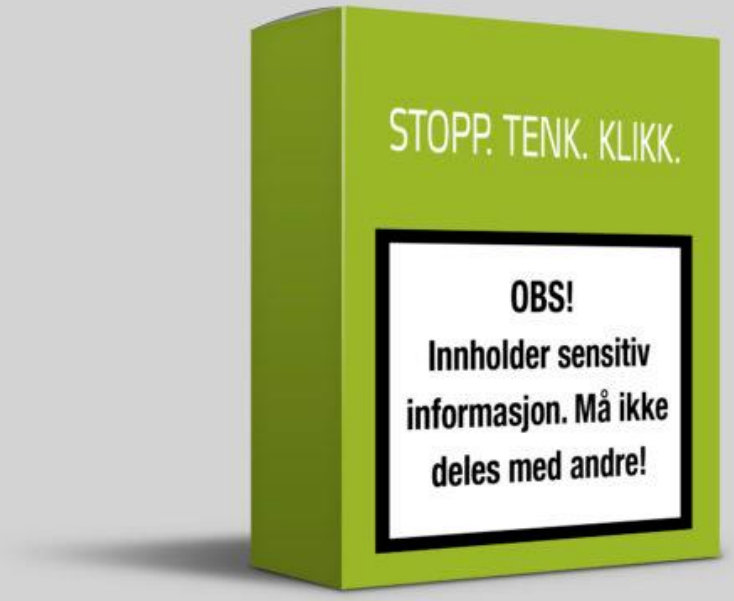

4human
We simplify and improve!

Innføring av 2-faktor autentisering ved pålogging
- for kunder som benytter Evolution -

Målsetning med presentasjon:

Øke kunders kompetanse om riktig valg av sikring av persondata ved bruk av 1- eller 2-faktor autentisering

Versjon 1.0 - 24. februar 2017



4human

Formålet med denne presentasjon er å informere om:

- Hva er ‘autentisering’?
  - Beskrivelse av 2-faktor versus 1-faktor pålogging
- Hva tilbyr 4human for å øke sikkerheten ved pålogging?
  - 1-faktor sikkerhetsfunksjoner i kombinasjon med 2-faktor autentisering
- Hva anbefaler 4human ovenfor sine kunder?
  - Retningslinjer ovenfor nye kunder som skal implementeres
  - Retningslinjer ovenfor eksisterende kunder med 1-faktor
- Hvordan aktivere, bruke og deaktivere 2-faktor autentisering?
  - Hvordan aktivere 2-faktor autentisering for kunder?
  - Hvordan forberede brukere for å logge på etter aktivering av 2-faktor
  - Hvordan gjennomføre førstegangs pålogging for brukere?
  - Hva må gjennomføres hvis bruker bytter mobiltelefon?
  - Hvordan deaktivere 2-faktor autentisering for kunder?

1. Hva er AUTENTISERING?

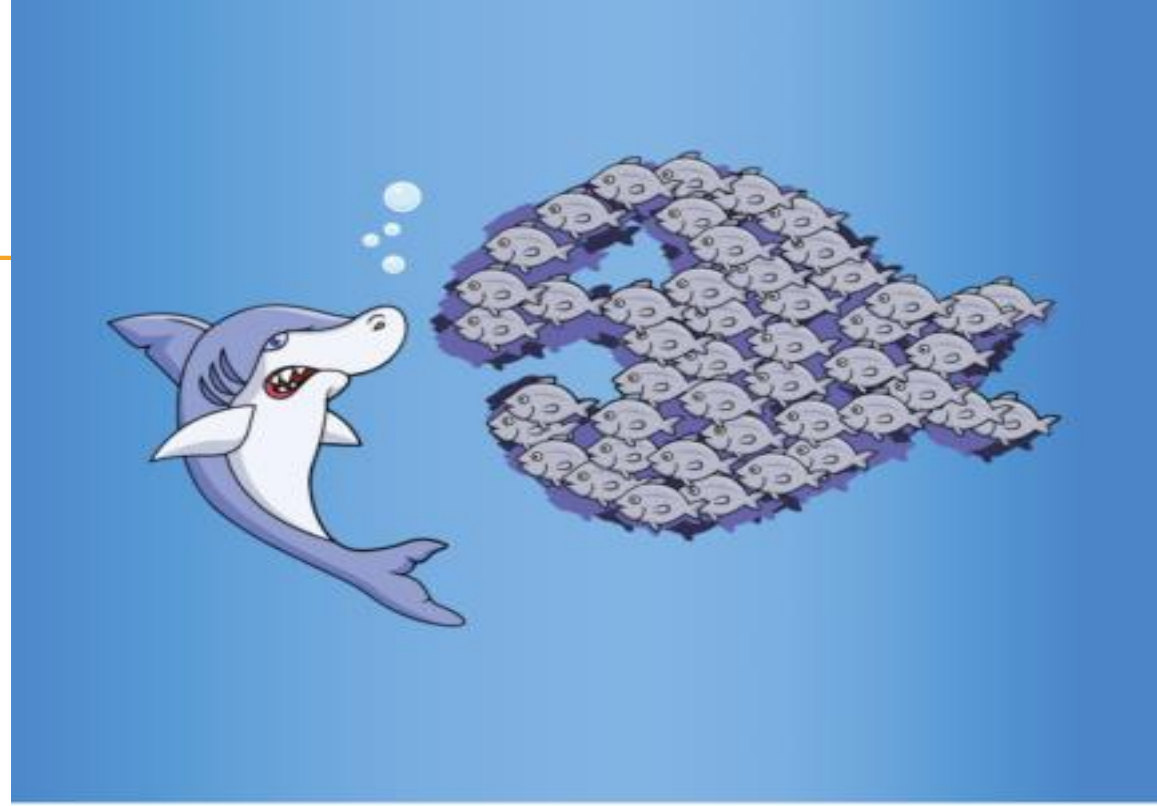
- **De fleste av oss bruker en eller flere av disse 2-faktor mekanismene i dag**:
  - BankID (kodegenerator/mobil), BuyPass (mobil/smartkort), MinID (sms) og Commfides (USB-pinne)
  - Med referanse til tyverier av ID og passord fra populære skytjenester og bruk av samme ID (mail-adresse) og tendens til gjenbruk av passord

- **Presentasjon av 2-faktor autentisering - fra SANS Institute**
  - Oversatt til norsk av NorSIS – Norsk Senter for Informasjonssikring

- **De mest vanlige risiko-faktorer ved lav sikkerhet med 1-faktor autentisering:**
  - Låne passord til kollega med gode intensjoner
  - Kollega 'ser' passord ved din pålogging
  - Passord knekkes av nett-tjeneste/robot
  - Bruk på passord som er lett å huske (hund, ektefelle/barns navn, fødeår, bilmerke etc)
  - Samme passord gjenbrukes ved 'endring' av passord
  - Brukerkonto som ikke blir stengt etter fratredelser eller sikring av midlertidige brukerkonti (eksterne)

4human tilbyr aktivering av 2-faktor autentisering fra onsdag 01.03.2017 – Kunden vil bli belastet for 1 time bistand ved aktivering og deaktivering.

Ta kontakt med 4human Brukerstøtte via vårt kundesenter evo.zendesk.com eller melding til support@4humanhrm.no



Du er en viktig del av virksomhetens forsvar mot datakriminalitet.
Sammen står vi sterkere!

NorSIS

2. Hva **tilbyr** 4human for å øke sikkerheten ved pålogging?

- Eksisterende funksjonalitet i Evolution ved 1-faktor autentisering av bruker
  - Superbruker kan tvinge Bruker til å bytte passord ved neste forsøk på innlogging
  - Superbruker kan opprette midlertidig BrukerID /endre en BrukerID (i oppsigelsestid) til å ha en definitiv utløpsdato og deretter blir konto deaktivert.
  - Superbruker kan iverksette sjekk av nytt passord mot tidligere versjoner av passordet
  - Superbruker kan aktivere en funksjon som gjør en Brukerkonto stenges når det er utført 5 påloggingsforsøk som feiler,
  - Superbruker kan tvinge bruker til å benytte et sammensatt passord (eksempel: RtUvLy7) med visst antall karakterer, store/små bokstaver og tall
  - Superbruker kan sørge for at en brukerkonto som ikke vært pålogget siste NN dager blir deaktivert ved neste forsøk på pålogging.
- Superbruker kan avgrense pålogging til kun å fungere innenfor bedriftens eget nettverk
  - Ved å legge inn tillatte ip-adresser (kontakt IT-ansvarlig)

2. Hva **tilbyr** 4human for å øke sikkerheten ved pålogging? (forts)

- Innføring av 2-faktor autentisering
  - Forsterker/øker sikkerhetsnivået i kombinasjon med 1-faktor autentisering
  - Dette vil gjelde for bruk via PC og nettbrett/mobiltelefon
  - To-stegs verifisering av Bruker ved bruk av 3.parts tjeneste med bruk av app'er i mobiltelefonen:
    - Google Authentication for iPhone og Android
    - Authenticator for Windows-telefoner
  - To-stegs verifisering av bruker ved bruk av 3.parts tjeneste (WinAuth) for Windows-pc'er

Har du sikret informasjonen din?

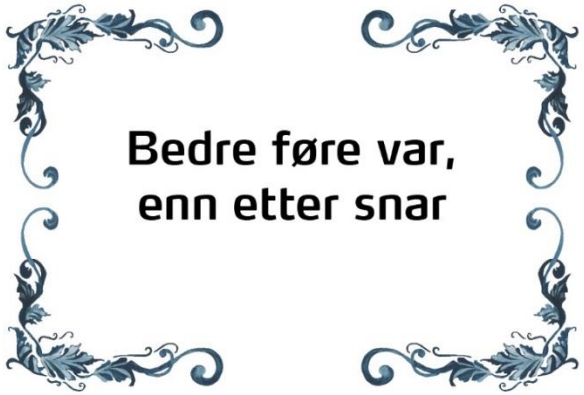
3. Hva **anbefaler** 4human ovenfor sine kunder?

- 4human anbefaler alle kunder å benytte 2-faktor autentisering ved pålogging
  - Bakgrunn for dette er økende krav til sikring av persondata og tydeliggjør ansvaret for både kunden (som *behandlingsansvarlig)* og 4human som *databehandler* for kunden).
  - Ny personopplysningslov fra mai 2018 med bakgrunn i EU's General Data Protection Regulation (GDPR) – vil antagelig gjelde for bedrifter med mer enn 250 ansatte.
  - Det er ikke et krav fra offentlige instanser/tilsynsmyndigheter om å innføre 2-faktor men en mulighet til å bedre sikkerheten for persondataene.
  - Det er ikke nødvendig å innføre 2-faktor autentisering for kunder som kun bruker elektroniske håndbøker i Evolution

3. Hva **anbefaler** 4human ovenfor sine kunder? (forts)

- For nye kunder
  - Så vil 4human aktivere 2-faktor ved generering av kundens instans (URL)
  - Endring tilbake til 1-faktor må avklares/signeres på i Oppstartsdokumentet

- For eksisterende kunder
  - Så vil 4human anbefale at disse går over til 2-faktor autentisering
  - Dette budskapet vil bli repetert i nyhetsbrev/sikkerhetspresentasjoner/på brukerkonferanser
  - Kunder må allikevel på et selvstendig grunnlag vurdere dette med utgangspunkt i egen bedrifts operative situasjon (IT-miljø/sikkerhetskrav)



4. Hvordan **aktivere**, bruke og deaktivere 2-faktor autentisering?

1. Hvordan **aktivere** 2-faktor autentisering for eksisterende kunder?
    1. Kunden må sende skriftlig bestilling til 4human's kundestøtte (via e-mail eller Zendesk) for å få aktivert 2-faktor autentisering på et gitt tidspunkt. Denne bestillingen skal komme fra Superbruker/Kontraktsansvarlig hos kunden.
    2. 4human bekrefter mottak av bestilling, sender bekreftelse tilbake med relevant dokumentasjon og oppdaterer saken i Support-systemet.
    3. 4human sender påminnelse til kunden ett antall dager/timer før aktivering slik at kunden kan melde tilbake at de er klare (etter interne forberedelser)
    4. Avvente bekreftelse fra kunde om **Ja** eller **Nei** på aktivering på gitt tidspunkt
    5. Basert på respons fra kunden:
        i. Aktivere 2-faktor på avtalt tidspunkt eller avvente aktivering til nytt tidspunkt

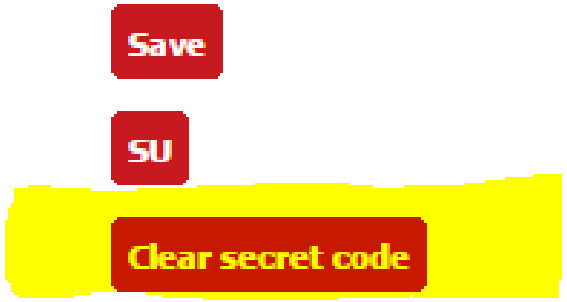
4. Hvordan **aktivere,** bruke og deaktivere 2-faktor autentisering? (forts.)

- Hvordan bør Superbruker **forberede** sine brukere for å logge på etter aktivering av 2-faktor?
  - Superbruker må informere sine brukere om at aktivering av 2-faktor pålogging er besluttet gjennomført av arbeidsgiver/selskapet.
  - Informere brukere om hvilke sikkerhetsfunksjoner* (1-faktor og 2-faktor) som er tilgjengelig og hvilke valg som bedriften har valgt å benytte.
  - Bistå egne brukere med nedlasting* av app'er for 2-faktor autentisering
  - Følge opp brukere etter at 4human har aktivert 2-faktor for bedriften.

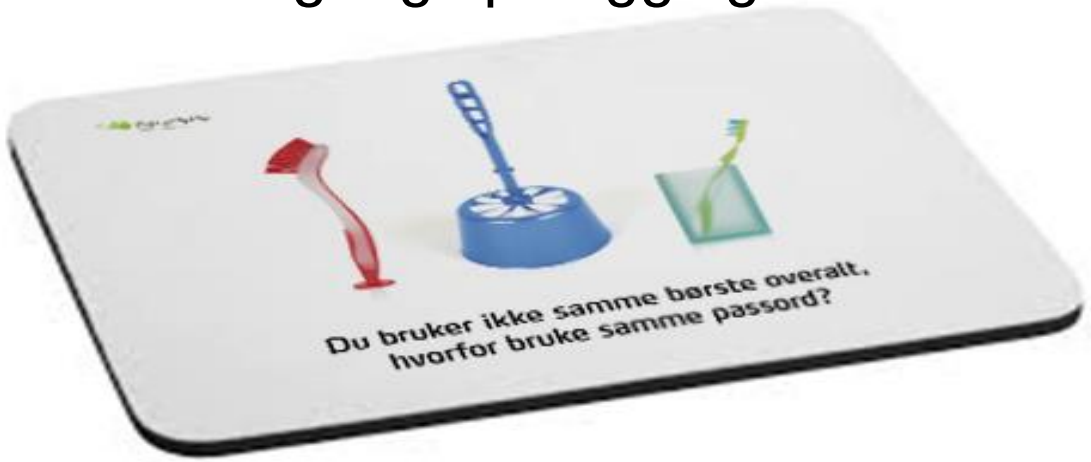
- Det er laget dokumenter som vil bli gjort tilgjengelig for nedlasting fra kundesenteret.
  - Denne presentasjonen
  - Orientering om 2-faktor autentisering fra Sans Institute (norSIS)
  - Sikkerhetsfunksjoner for 1-faktor autentisering
  - Førstegangs pålogging ved aktivering av 2-faktor autentisering

4. Hvordan aktivere**, bruke** og deaktivere 2-faktor autentisering? (forts)

- Hva må gjennomføres hvis bruker **bytter telefon**?
  - Bruker må laste ned <*riktig app ifht type OS på mobilen*> til ny mobil
  - Superbruker må resette hemmelig kode i brukerens profil i Evolution



  - Bruker må gjennomføre prosedyre som for førstegangs pålogging



4. Hvordan aktivere, bruke og **deaktivere** 2-faktor autentisering? (forts)

- Hvordan deaktivere 2-faktor autentisering for kunder?
  1. Kunden sender skriftlig bestilling til 4humans brukerstøtte for å deaktivere 2-faktor med en gitt dato/tidspunkt– denne må komme fra en autorisert person (superbruker/kontraktsansvarlig).
  2. 4human bekrefter at 2-faktor vil bli deaktivert på avtalt dato/tidspunkt
  3. 4human oppdaterer Support-systemet vedr. anmodning om deaktivering og lagrer e-post fra kunden.
  4. Kunde informerer sine ansatte om deaktivering av 2-faktor.
  5. 4human deaktiverer 2-faktor for kundens instans og sender bekreftelse til kundens representant.

5. Oppsummering

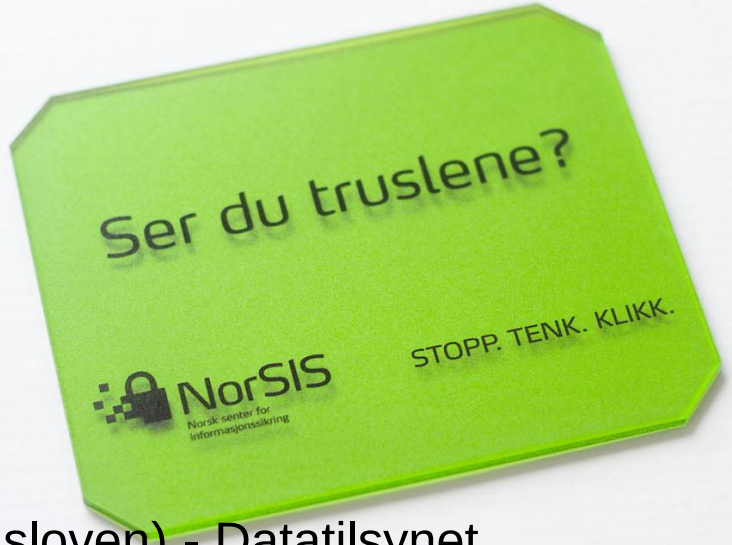
1. 4human introduserer mulighet for aktivering av 2-faktor autentisering ved pålogging – ved bruk av koder fra app'er i mobil eller applikasjon lastet ned på PC.

2. For eksisterende kunder – så vil 4human anbefale at disse øker sitt sikkerhetsnivå ved å aktivere 2-faktor autentisering for sine brukere. Kunder må vurderer dette på selvstendig grunnlag og ihht. egen bedrifts operative situasjon (IT-miljø/sikkerhetskrav).

3. For nye kunder – så vil 4human aktivere 2-faktor ved etablering av ny kundeinstans. Kunden kan beslutte tilbakestilling til kun 1-faktor autentisering gjennom oppdatering/signering av oppstartsdokument før implementering starter.

Linker til relevante informasjonskilder / Informasjonssikkerhet

- Sans Institute/norSIS: 'Sikker autentisering'
- Sikkert.no: 'Nasjonal sikkerhetsmåned – oktober'
- Link til Norsk Senter for InformasjonsSikring (norSIS)
  - Mulighet for ukentlig nyhetsbrev
  - Nettbutikk med diverse produkter (bildene i presentasjon)
- Nettvett fra norSIS:
  - 'Aktiver 2-faktor bekreftelse' / 'Slik lager du sterke passord'
  - 'Sikker pålogging'



- Lov om behandling av personopplysninger (personopplysningsloven) - Datatilsynet
- Sikkerhetsbestemmelsene i personopplysningsforskriften - Datatilsynet
- Databehandleravtale om behandling av personopplysninger – Datatilsynet
- Ny forordning om behandling av personopplysninger (GDPR) – Datatilsynet
- EU General Data Protection Regulation (GDPR) som iverksettes fra mai 2018

Speil til salgs hos norSIS