Installer ny app efter sommerferien, hvis du fortsat vil læse arbejdsmail på din private telefon

For at beskytte data skal du fremover bruge to nye apps. Til gengæld kan du så bruge private enheder til at læse arbejdsmails.

Region Hovedstaden oplever, som mange andre organisationer, at cyber-angreb er en stigende trussel. Derfor er det nødvendigt at lægge et ekstra sikkerhedslag på adgangen til din arbejdsmail fra mobil og på adgangen til webmail, når du ikke er på en regionscomputer.

Der lukkes for at modtage arbejdsmails på private enheder på den nuværende måde **d. 14. august 2018.**

Hvis du vil forsætte med at læse arbejdsmails som hidtil, skal du tilmelde dig to apps. De to apps, som du skal tilmelde dig **efter d. 14. august 2018**, hedder MobileIron og Entrust.
Det er relevant, hvis du læser arbejdsmails fra:

- Privat telefon eller tablet
- Regionens telefoner og tablets
- Mobile enheder der er på andre netværk end regionens eget

MobileIron og Entrust hjælper med sikkerheden på to forskellige måder:

MobileIron: Giver mulighed for at få arbejdsmail og kalender ind på en privat eller regionsejet mobil/tablet i dens eget standard-mailprogram.

Behovet for øget sikkerhed betyder, at regionen via MobileIron administrerer enhedens sikkerhed og vil kunne fjerne arbejdsmæssigt indhold på telefonen i tilfælde af sikkerhedsbrud.
Regionen kan IKKE se private ting som dine apps, samtaler, mails, kontakter, kalender, sms'er mv. Regionen kan kun se oplysninger, der relaterer sig til model, softwareversion, brugerens navn, primære mail-adresse samt mobilnummer.

Entrust: Giver mulighed for at tilgå regionens data og systemer fra din private enhed udenfor regionens netværk, hvis enheden ikke er registreret i MobileIron.

Den øgede sikkerhed betyder, at du får et ekstra login – en sikkerhedskode - som sendes til en telefon/tablet via en app, hver gang, du f.eks. logger ind på din webmail. Hermed er der to-faktor autentifikation på tilgangen, hvilket øger sikkerheden markant.

Sådan gør du, når du skal installere de nødvendige apps efter d. 14. august 2018.

Jeg vil have mine arbejdsmails ind i min private telefon/tablets mailprogram

Du installerer MobileIron via portalen, som bliver aktiv efter d. 14. august 2018.:

- https://temm.regionh.dk

Så kan du anvende arbejdsmails, kalender, noter, kontakter og påmindelser via telefonens installerede mailprogram.

Se manualer og brugervejledninger til MobileIron her:

- Manualer til MobileIron, information om support, versionskrav m.m.

Jeg vil *ikke* installere MobileIron på min private telefon/tablet, men stadig kunne læse arbejdsmails

Du installerer Entrust ved at følge vejledningen, som findes her:

- Vejledning til opsætning af Entrust

Så kan du tilgå arbejdsmails ved at åbne din browser på mobilen, og skrive adressen:

- https://outlook.office365.com

i adressefeltet og logge ind med dit Region H-login og dernæst den ekstra kode, som du modtager fra Entrust.

Jeg læser arbejdsmails på en RegionH-ejet telefon/tablet

Du skal tjekke om din telefon er registreret i MobileIron. Søg på MobileIron på telefonen og se, om appen allerede findes. Hvis MobileIron allerede er installeret på din telefon, er enheden registeret og du kan tilgå din arbejdsmail (Exchange konto) og skal derfor ikke gøre yderligere.

Hvis MobileIron ikke er installeret, skal du oprette en sag i **CIMT Serviceportal (Meld fejl -> Andet -> Andre fejlmeldinger)**

Jeg har brug for at læse webmail fra min private PC uden for Region H-netværk

Du skal tilmelde dig Entrust. Det medvirker, at hver gang du logger på med dit brugernavn og password, skal du også bruge en ekstra kode til din telefon/tablet (privat eller regionsejet), som du så taster ind i forlængelse af dit normale brugernavn og password.
Det kræver, at du installerer Entrust på en mobil enhed, som du har på dig.

Jeg har brug for at læse webmail fra min RegionH-ejede PC udenfor Region H-netværk

Kombinationen af brugernavn/password, samt GlobalProtect på RegH PC'en, er en to-faktorløsning i sig selv. Det betyder derfor, at PC'en altid er på et internt netværk og derfor ikke har behov for den ekstra autentifikation.

De systemer der fra d. 14. august 2018 kræver, at du er tilmeldt Entrust er webmail (Exchange konto), og ServiceNow. Med tiden vil flere løsninger blive omfattet.

Har du spørgsmål

Læs vejledningerne igennem, som du finder via intranettet her:

- MobileIron på intranettet
- Entrust på intranettet

Her vil du også kunne finde svar på spørgsmål om support, versionskrav m.m.
Ret henvendelse til CIMT Service, hvis du har yderligere spørgsmål.

Mere om cyber-angreb og sikkerhed

Det er det øgede trusselsbillede, der medfører, at Center for It, Medico og Telefoni (CIMT) har sat øget fokus på at sikre Region Hovedstadens informationssikkerhed.

I situationer, hvor data tilgås fra eksterne netværk og lokationer er risikoen for at få kompromitteret data betydeligt større end indenfor Region Hovedstadens eget netværk. Når der ikke er kontrol over de enheder, der bruges til at tilgå systemerne, kan det potentielt give ukendte personer adgang.

Hvordan sikrer MobileIron adgangen

Hvis du bruger din private telefon eller anden enhed, så skal CIMT have styr på hvilke enheder, som synkroniserer med regionens mailsystem, så uønskede personer ikke får adgang til Region Hovedstadens data.

CIMT ønsker at kende:

- Den mobile enhed og hvem, som er logget på mailprogrammet
- Sikre, at der er låsekode på enheden
- Sikre at enheden er krypteret
- Kender enhedens styresystem

Når du registrerer din enhed i MobileIron, bliver din enhed underlagt følgende forhold:

- Pinkoden vil fremover som krav være på 6 "ikke simple"-cifre, hævet fra kravet om 4 "simple" cifre.
- Antal mislykkede login-forsøg før alt på enheden slettes ændres fra 6 til 10 forsøg.
- Enheden skal krypteres (de fleste enheder er allerede krypteret automatisk).
- Region Hovedstaden kan se dit brugernavn, de indstillinger, der kommer fra MobileIron samt grundlæggende oplysninger om din mobil så som model mv.

Ovenstående forhold gælder både private enheder og Region H-ejede enheder, der er registreret i MobileIron.

Det skal bemærkes, at brugeren ved installationen af MobileIron på sin enhed giver adgang til, at Region Hovedstaden administrerer enhedens sikkerhed og vil kunne fjerne arbejdsmæssigt indhold på telefonen i tilfælde af sikkerhedsbrud. Sikkerhedsbrud kan f.eks. være hvis brugerens ansættelsesforhold ophører eller at enheden ikke overholder minimumsgrænsen for styresystemets version. Dette gælder også Region H-ejede enheder.