Notat - innføring av Windows Hello for Business

Dette notatet er et arbeidsnotat som samler relevante vurderingspunkter i forbindelse med innføring av Windows Hello for Business i kommunesektoren.

Generelt om Windows Hello for Business

Windows Hello for Business (WHfB) er en biometrisk autentiseringsløsning som følger med operativsystemet Windows 10/11, og som blant annet kan autentisere brukere med fingeravtrykksavlesing eller ansiktsgjenkjenning. Med Windows Hello logger ikke brukerne inn på sin datamaskin med sitt passord, men med sine biometriske opplysninger. Brukeropplevelsen med WHfB blir altså det samme som når vi bruker Face ID på iPhone.

WHfB er en sterk autentiseringsmetode som kombinerer noe *brukeren har* (sin egen datamaskin) med noe *brukeren er* (sine biometriske opplysninger). Siden brukeren ikke lengre forholder seg til sitt eget passord, så er denne autentiseringsmetoden såkalt *phishing resistant*. Det er med andre ord ikke mulig for en trusselaktør å lure passordet fra brukeren, fordi brukeren ikke har et passord å gi fra seg. Andre passordløse autentiseringsmetoder er FIDO2 og sertifikatbasert autentisering.

WHfB bruker asymmetriske krypteringsnøkler som er beskyttet av TPM-modulen på brukerens datamaskin. En TPM-modul (Trusted Platform Module) er en sikkerhetsenhet installert i datamaskinen, og som brukes for å lagre sensitiv informasjon (som biometriske opplysninger).

Generelt om biometri til autentiseringsformål

Biometrisk autentisering handler om å måle biometriske kjennetegn for å identifisere eller verifisere en person. Identifisering handler om å fastslå en persons identitet, det vil si å gjenkjenne en person blant flere mulige personer (en-til-mange forhold). Verifisering handler om å sjekke om personen er den han eller hun utgir seg for å være (en-til-en forhold). Generelt sett regnes biometri brukt til verifisering som mindre inngripende enn biometri brukt til identisering. Bruk av biometri til autentiseringsformål er et eksempel på verifisering.

Informasjonssikkerhetsrisikoer ved bruk av WHfB

Risiko for falske autentiseringer
Feilratene i biometriske løsninger uttrykkes med FAR (False Acceptanse Rate) og FRR (False Rejection Rate). Kravet til maksimal FAR for WHfB er på 0,001 prosent. Det betyr at Windows Hello maksimalt kan autentisere feil person i 1 av 10.000 autentiseringer. I realiteten må en ansatt ha mange likhetstrekk med den autentiserte personen før en slik falsk autentisering kan skje. De «gamle» angrepsmetodene, som å vise et bilde av brukeren, fungerer ikke lengre. Kameraet bruker blant annet infrarødt lys for å avdekke dybdeforskjeller. Risikoen for falske autentiseringer vurderes som lav.

Risiko for datalekkasje
De biometriske opplysningene blir lagret som en datarepresentasjon av brukerens ansikt. Det er ikke mulig å reversere denne representasjonen til et bilde som uttrykker brukeren. Selv om en angriper klarer å hente ut denne datarepresentasjonen, så kan ikke den brukes til å forfalske autentiseringer. Risikoen for datalekkasje vurderes derfor som lav.

Risiko for tap eller tyveri av datamaskinen
Det finnes enkelte angrepskonsepter som forsøker å kompromittere Windows Hello, for eksempel ved å sette opp et ekstra webkamera, men metodene er forholdsvis kompliserte. Hvis datamaskinen er kryptert med BitLocker vurderes risikoen for fysiske angrep som lav.

Ansiktsverifisering og forholdet til personvernregelverket

Personopplysningsloven § 12 setter krav til bruk av fødselsnummer og andre entydige identifikasjonsmidler. Slik informasjon kan bare behandles når det er saklig behov for sikker identifisering, og metoden er nødvendig for å oppnå slik identifisering. Entydige identifikasjonsmidler omfatter bruk av biometri, jf PVN 2006-7 (fingeravtrykksavlesning i Tysvær kommune) og 2006-10 (fingeravtrykksavlesning i Esso Norge AS). Merk at disse avgjørelsene er tatt før GDPR ble lovfestet, men antas overførbart til nytt lovverk.

Biometriske opplysninger vurderes å være en personopplysning, jf GDPR artikkel 4 punkt 1. Innsamling og prosessering av slik informasjon vurderes å være en behandling, jf GDPR artikkel 4 punkt 2. Biometri vurderes å være spesielle kategorier personopplysninger, jf GDPR artikkel 9 punkt 1. Bruk av WHfB må følgelig gjennomføres innenfor rammene til GDPR. Det innebærer blant annet:

1. Kommunen må vurdere det saklige behovet for sikker identifisering, jf POL § 12. Her er det viktig at kommunen definerer formålet med å ta i bruk WHfB. Hvis formålet er basert på at det skal være enklere for brukerne å logge inn, så er det vanskelig å se for seg at tiltaket er nødvendig. Hvis formålet er basert på en sikkerhetsvurdering hvor svak autentisering (brukernavn og passord) anses å resultere i for lav informasjonssikkerhet, så kan det være aktuelt å vurdere sterkere autentiseringsformer.
2. Kommunen må vurdere hvorvidt metoden er nødvendig for å oppnå sikker identifsering, jf POL § 12. Det finnes som nevnt alternative sikre autentiseringsmetoder, som FIDO2 og sertifikatbasert autentisering. En utfordring med FIDO2 er at brukeren kan miste FIDO2-enheten (som oftest en USB-enhet).
3. Kommunen må finne et gyldig rettslig grunnlag, jf GDPR artikkel 5.
4. Kommunen må finne et gyldig vilkår for å behandle slike spesielle kategorier personopplysninger, jf GDPR artikkel 9 punkt 2.
5. Kommunen må gjennomføre ROS etter GDPR artikkel 32.
6. Kommunen må gjennomføre DPIA etter GDPR artikkel 35. Relevante kriterier fra atikkel 29-gruppens kriteriesett er særlige kategorier og mange registrerte.

Biometrisk autentisering kan med andre ord være et relevant eksempel på sterk autentisering, men kommunen bør i sine risikovurderinger vurdere om det finnes mindre inngripende autentiseringsmetoder. Autentisering med Microsoft Authenticator kan være et alternativ, men merk at også her brukes biometri (ansiktsgjenkjenning).

Oppsummert vurderes WHfB å være en tjeneste forbundet med god informasjonssikkerhet, men hvor det må gjøres nærmere vurderinger av hvordan tjenesten kan tas i bruk innenfor rammen av personvernregelverket. I den forbindelse fremmes tre forhold til diskusjon:

Avklaring 1 – Omfattes ansiktsverifisering med WHfB av personvernregelverket?

Datarepresentasjonen av brukernes biometriske opplysninger lagres lokalt på brukerens egen datamaskin. Datarepresentasjonen kan ikke reverseres til et format som kan gjenkjennes av den biometriske sensoren i kameraet. Representasjonen lagres som et asymmetrisk nøkkelpar. Det kan argumenteres for at denne dataen ikke omfattes av definisjonen av personopplysninger og biometriske opplysninger i GDPR artikkel 4.

Det pågår for tiden et sandkasseprosjekt som utforsker mulighetene for ansiktsgjenkjenning uten at det regnes som biometri, se https://www.datatilsynet.no/regelverk-og-verktoy/sandkasse-for-kunstig-intelligens/pagaende-prosjekter2/salt-mobai-m.fl/. Prosjektet vil kunne bidra med avklaringer for hvorvidt det er mulig å implementere tekniske løsninger for ansiktsverifisering uten at det anses som en behandling etter personvernregelverket.

Avklaring 2 – hvilket rettslig grunnlag i artikkel 6 kan brukes?

Mulige relevante grunnlag kan være avtale (arbeidsavtale), samtykke, rettslig forpliktelse (eforvaltningsloven) eller berettiget interesse.

Når det gjelder rettslig forpliktelse, så finnes det flere lover som regulerer informasjonssikkerhet i kommunal sektor, blant annet eforvaltningsforskriften (som stiller krav til internkontroll på informasjonssikkerhetsområdet), og GDPR (som stiller krav til personopplysningssikkerhet). Felles for disse er at de tar utgangspunkt i at kommunen selv gjennomfører risikovurderinger og implementerer tiltak for å nå et tilstrekkelig sikkerhetsnivå.

Når det gjelder samtykke, så egner det seg som utgangspunkt ikke som rettslig grunnlag i forholdet arbeidsgiver-arbeidstaker, men det bør være mulig å sikre et frivillig og gyldig samtykke dersom det finnes et fullgodt alternativ til WHfB. Brukerne kunne for eksempel fått valget mellom å bruke WHfB eller FIDO2. Dette kan imidlertid føre til administrativt merarbeid, blant annet i forbindelse med innhenting av samtykker og teknisk tilrettelegging av autentiseringsmetodene på brukernivå.

Avklaring 3 - hvilket vilkår i artikkel 9 kan brukes?

Et mulig vilkår kan være at behandlingen er nødvendig for at den behandlingsansvarlige skal kunne oppfylle sine forpliktelser og utøve særlige rettigheter på området arbeidsrett, trygderett og sosialrett. Et annet mulig vilkår kan være samtykke.

20.12.23

Roy Allan Hansen
sjefskonsulent Move AS