Risiko- og sårbarhetsanalyse i forbindelse med bruker med begrenset tilgang for inn- og utregistrering

Sist revidert av Kristoffer Iversen 29.07.19

Innledning

Alle virksomheter er forpliktet til å gjennomføre risikovurderinger av informasjonssikkerheten ved behandling av personopplysninger. Med informasjonssikkerhet menes evnen til å forebygge, avdekke og håndtere hendelser som kan føre til brudd på personopplysningenes konfidensialitet, integritet eller tilgjengelighet.[1] Arbeidet med risikovurderinger er derfor en viktig del av institusjonenes ledelsessystem for informasjonssikkerhet.

Når risikovurderingen er gjennomført, er det viktig å iverksette tiltak som reduserer risikoen for hendelser med uakseptabel høy risiko. Dette beskrives ofte som risikohåndtering.

Risikovurderinger skal også gjennomføres ved endringer som kan ha betydning for informasjonssikkerheten. Endringer kan være at det tas i bruk nye underleverandører, det skjer endringer i driftsopplegget eller at funksjonaliteten i tjenesten endres eller utvides.

Nye risikovurderinger kan gjennomføres ved at tidligere vurderinger revideres og oppdateres.

Formål

I denne analysen gjøres det rede for de viktigste uønskede hendelser som kan føre til brudd på informasjonssikkerheten når det gjelder bruk av bruker *med begrenset tilgang* for inn- og utregistrering i Vigilo. Slike hendelser skal avdekkes og vurderes i risikovurderinger. For hver vurdering har vi en egen vurdering over tiltak som er iverksatt for å redusere denne risikoen.

Bakgrunn

Vigilo har i over lang tid drøftet mulighetene og konsekvensene av å opprette en brukerrolle med begrenset tilgang for ansatte i barnehage og SFO for administrering av inn- og utregistrering av barn sammen med våre kunder og brukere.

Gjennom direkte tilbakemelding fra kunder og brukere har Vigilo fått tilbakemelding på at det i daglig praksis vil være svært vanskelig å administrere inn- og utregistrering av barn når hver enkelt ansatt må bruke sin egen konto og derav også egen innlogging for dette formålet.

Kundene våre rapporterer om at det lages alternative rutiner i barnehagene som øker uønsket risiko for informasjonssikkerheten til barna og foresatte ved enhetene. Det rapporteres om at én eller flere brukere gir fra seg sin innloggingsinformasjon og at denne kontoen dermed blir 'felles' og blir benyttet som en fellesbruker til inn- og utregistrering. Det rapporteres også om at enhetene lar være å føre inn- og utregistrering i nåtid, men samler registreringen til et tidspunkt i løpet av dagen. Ingen av de overnevnte alternative tiltakene er ønskelige.

Basert på dette har Vigilo lagt til rette for å oprette en bruker med svært begrensede muligheter for innsyn og handling. **Denne brukeren har kun en rolle som kun vil ha anledning til å se følgende informasjon om barn på sin enhet: Bilde, fullt navn, status (sjekket inn, sjekket ut, venter på og fravær) og klokkeslett for siste registrering. Brukeren vil ikke ha anledning til å se historiske registeringer eller forventet fravær frem i tid. Handlingen brukeren kan foreta seg er kun å endre status på barnet.**

[1] Konfidensialitet: Hindre uvedkommende i å få tilgang til informasjon.

Integritet: Hindre uautorisert endring og sletting av informasjon.

Tilgjengelighet: Sørge for at autoriserte personer får tilgang til informasjon, når de har behov for det.

Rent praktisk vi hver enhet opprette en fiktiv bruker som de ansatte kjenner brukernavn og passord til. Denne fiktive brukeren har kun én rolle, med begrenset tilgang og vil kun kunne se og behandle overnevnte opplysninger.

Vigilo mener med dette at avveiningen mellom brukervennlighet og barnas informasjonssikkerhet gjennom denne analysen er vurdert. Med bakgrunn i kundenes ønske, rapportene om alternative rutiner og de begrensede innsyns- og behandlingsmulighetene en bruker med begrenset tilgang vil ha, mener vi at en slik brukerrolle for inn- og utregistrering er hensiktsmessig og vil ivareta informasjonssikkerheten til barna og deres foresatte.

Vurdering

Sannsynligheten for at hendelser skjer vurderes på en skala fra 1-5, og konsekvensen av at hendelsen skjer vurderes også på en skala fra 1-5. Risikoen (**R**) beregnes ved i hendelsestabellen ved å multiplisere konsekvensen (**K**) med sannsynligheten (**S**).

Konsekvens: Sannsynlighet:	1. Ubetydelig	2. Mindre alvorlig	3. Betydelig	4. Alvorlig	5. Svært alvorlig
5. Svært sannsynlig/kontinuerlig	**5**	**10**	**15**	**20**	**25**
4. Meget sannsynlig/periodevis, lengre varighet	**4**	**8**	**12**	**16**	**20**
3. Sannsynlig/flere enkelttilfeller	**3**	**6**	**9**	**12**	**15**
2. Mindre sannsynlig/kjenner tilfeller	**2**	**4**	**6**	**8**	**10**
1, Lite sannsynlig/ingen tilfeller	**1**	**2**	**3**	**4**	**5**

Hendelser

Hendelse 1:	Uvedkommende får tilgang til konto
Hva kan skje?	Uvedkommende kan få tilgang til konto
Årsak:	Dårlige holdninger ved bruk av passord og pålogging. Eksempelvis når dette ligger synlig en plass ved enheten slik at foresatte eller andre ser opplysningene, eller ved at tidligere medarbeidere fortsatt har tilgang til brukernavn og passord.
Tiltak:	- Gode rutiner på oppbevaring og tilgjengelighet for brukernavn og passord. - Sterkt passord - Regelmessig endring av passord
Vigilos vurdering:	Vigilo kan lite gjøre med brukeres håndtering av passord og pålogging, annet enn å veilede og gi råd. Brukernavn og passord skal endres med jevne mellomrom uavhengig om det er endringer i personalet eller ikke. S:3 K:2 **R:6**
Antatt risiko:	Middels

Hendelse 2:	Uvedkommende får se nåtidsstatus ved enhet
Hva kan skje?	Uvedkommende kan ved levering/henting se på skjerm hvem som er hentet/levert og når.
Årsak:	For eksempel dårlige holdninger ved å sette skjerm i dvale.
Tiltak:	- Rutiner - Opplæring
Vigilos vurdering:	Vigilo kan lite gjøre med brukeres håndtering av visning av personopplysninger, annet enn å veilede og gi råd. Alle opplysninger om barn bør skjermes for uvedkommende. S:3 K:1 **R:3**
Antatt risiko:	Lav

Hendelse 3:	Autorisert brukerfeil
Hva kan skje?	Ansatte i Vigilo (også underleverandører) eller brukere med nødvendige tilganger ved uhell gjør feil slik at informasjon blir tilgjengelig for personer som ikke skal ha tilgang.
Årsak:	Manglende opplæring og oppfølging.
Tiltak:	- Rutiner - Opplæring - Tilgangsstyring
Vigilos vurdering:	Menneskelig svikt vil en aldri kunne utelukke. Vigilo har sterkt fokus på interne rutiner, tilgangsstyring og opplæring. Vigilo har også stort fokus på «riktig arbeid» i sin opplæring utad til brukere. Alle som har en bruker i Vigilo fra før har anledning til å drive inn- og utregistrering. Med det vil personene ikke få tilgang til å se eller behandle informasjon som de fra før ikke har tilgang til. S:2 K:2 **R:4**
Antatt risiko:	Lav

Hendelse 4:	Manglende administrering av brukertilganger
Hva kan skje?	Brukertilganger blir ikke endret eller avsluttet når personer (interne eller eksterne) skifter rolle, slutter eller av andre årsaker ikke lenger skal ha tilgang til data. Disse dataene kan dermed komme uvedkommende i hende. Ved brukerfeil eller manglende oppfølging av tilgangslister som brukeren selv har ansvar for, kan uvedkommende ha tilgang til opplysninger h*n ikke skulle hatt.
Årsak:	Brukertilganger og tilgangsstyring er delegert til flere roller i løsningen. Brukerne står i stor grad fritt til å tildele andre brukere rettigheter i et område.
Tiltak:	- Rutiner - Opplæring - Jevnlig oppfølging tilgangsrettigheter - Monitorering og logger
Vigilos vurdering:	Administratorer må påse at brukertilganger og roller stemmer overens med det som er det faktiske behovet ved sin enhet/sitt ansvarsområde. S:3 K:2 **R:6**
Antatt risiko:	Middels

Konklusjon

Denne risiko- og sikkerhetsvurderingen har gjennomgått fire potensielle, og de mest sannsynlige, hendelser knyttet til en bruker med begrenset tilgang for inn- og utregistrering av barn i Vigilo. Som vist i vurderingen er konsekvensene av feil/uønskede hendelser tilknyttet bruker med begrenset tilgang relativt begrensede. Dette på bakgrunn av at det er svært få opplysninger om barn man får tilgang til og enda færre opplysninger en kan behandle. Sannsynligheten for at uvedkommende får tilgang til opplysningene er større enn ved bruk av «normal» brukerhåndtering og pålogging. Dette på grunn av at brukernavn og passord er personlige, og at det benyttes sterk autentisering.

Konklusjonen er altså at en bruker med begrenset tilgang for inn- og utregistrering i Vigilo er sterkt ønsket av kundene og er vurdert som hensiktsmessig både fra kundene og Vigilo. De alternative rutinene som det rapporteres om vil i praksis føre til større risiko for informasjonssikkerheten til barna og deres foresatte enn ved opprettelsen og bruk av bruker med begrenset tilgang for inn- og utregistrering. Sannsynligheten for at andre enn autoriserte brukere får tilgang er større enn om man ikke hadde brukt en slik brukertilgang, men risikoen blir betydelig tatt ned da man begrenser innsyn og behandlingsmuligheter av opplysningene som ligger i Vigilo til et absolutt minimum.

Det er nødvendigvis slik at Vigilo, som alle andre tilbydere av IT-løsninger, aldri kan gi en 100 % sikkerhetsgaranti for at informasjon ikke kommer på avveie. Vigilo kan derimot garantere at vi tar informasjonssikkerheten på alvor og har de nødvendige systemer, rutiner, kompetanser og mottiltak klare for å forhindre/minimere konsekvensene ved en eventuell informasjonslekkasje.