Melding om avvik

Datatilsynet

Innsender

Organisasjonsnummer	833735462
Navn	WAYSCLOUD AS
Adresse	Postboks 2075 Vika
Postnr og sted	0125 OSLO

Melder din virksomhet dette avviket som behandlingsansvarlig eller databehandler? (●) Behandlingsansvarlig ( ) Databehandler

Beskrivelse av avviket

Hovedårsak til avviket: Brudd på rutiner

Tidsrom for avviket: 11/19/2024 til 11/19/2024

Når ble avviket oppdaget: 11/21/2024 Kl. 23:03:00

Angi hvor mange personer som kan være berørt av avviket: 76

Beskriv hva som har skjedd. Begrunn her om det er behov for å unnta fra offentlighet hele/deler av meldingen, og hvilke hjemler som ligger til grunn. Datatilsynet vil gjøre en selvstendig vurdering av dette.

Vårt selskap har engasjert sikkerhetsselskapet Fortified Technologies AS for å bistå med utarbeidelse av strategi og rammeverk knyttet til implementering og etterlevelse av CSF 2.0. I tillegg har selskapet bidratt på ad hoc-basis med ulike sikkerhetsrelaterte oppgaver, herunder vurdering av kandidater til stillingene som CISO og sikkerhetsarkitekt. De aktuelle dokumentene var lagret i et isolert filområde med strengt tilgangskontrollert autentisering, hvor kun tre ansatte i vårt selskap samt to eksterne konsulenter fra det nevnte sikkerhetsselskapet hadde tilgang.

Basert på loggene viser overvåkningssystemet at følgende handlinger fant sted den 19. november:
• Totalt 66 filer ble lastet ned manuelt av brukeren kn@fortified.no i tidsrommet kl. 17:23 til kl. 18:36.
Filene inkluderer:
• 32 PDF-filer
• 24 Microsoft Word-filer
• 5 Microsoft PowerPoint-filer
• 3 Google-dokumenter
• 2 Google-regneark
• Nedlastingene ble gjort med ulikt tidsintervall mellom hver handling, noe som indikerer at aktiviteten trolig ble utført bevisst.
• Hver fil ble lastet ned via nettleser etter autentisering, uten lokal synkronisering.

Hvordan oppstod avviket?

Brukeren har manuelt lastet ned filene gjennom sin nettleser, ved å logge seg inn i den aktuelle Google Disk-instansen og lastet ned filene over. Vi har vedlagt fullstendig logg over aktiviteten. Vi har valgt å sladde tittel og navn, men dokumentene kan identifiseres internt via oppslag på ID nummer.

Beskriv hva slags type personopplysninger som ble berørt av avviket

Kartleggingen pågår fortsatt, og vi vil så raskt som mulig gi en mer detaljert redegjørelse. Vi ser imidlertid med særlig bekymring på filer som omhandler jobbsøkere til stillingene som CISO og sikkerhetsarkitekt. Etter vår vurdering er dette stillinger som krever et høyt nivå av diskresjon og konfidensialitet.

De berørte filene inneholder blant annet:
• Søknadstekster og beskrivelser av kandidatens kompetanse.
• Oversikt over arbeidsroller kandidatene har hatt i større virksomheter, særlig innen sikkerhet.
• Referanser, vitnemål og andre utdanningsdokumenter.
• Personopplysninger som fødselsnummer og annen identifiserbar informasjon.

Vi ser alvorlig på at slike sensitive opplysninger kan ha blitt kompromittert og følger dette opp med høy prioritet.

Hvilken relasjon har virksomheten til de personene som er berørt av avviket?

22.11.2024 04:10:03 AR644275154

De berørte opplysningene gjelder primært jobbsøkere som har vært behandlet gjennom et eksternt rekrutteringsselskap. Leverandøren deltok i samtaler knyttet til risikovurdering og vurdering av kandidatenes erfaring og kvalifikasjoner.

Det finnes også dokumenter relatert til vår egen virksomhets infrastruktur blant materialet. Disse dokumentene ble imidlertid sladdet før de ble delt med leverandøren, og vi anser derfor at de ikke utgjør noen særlig risiko i dette tilfellet.

Beskriv hvor personopplysningene befinner seg etter avviket. Skriv også hvor mange og hvilken type mottakere som kan ha fått eller sett opplysningene.

Vi er i gang med kartleggingen og vil gi dere en oppdatering så snart som mulig. Det er sannsynlig at dokumentene fortsatt oppbevares hos leverandøren, og vi har ingen indikasjoner på at dette er gjort med onde hensikter. Likevel er det ingen legitim grunn til at dataene skulle lastes ned manuelt fra det etablerte diskområdet, da dette nettopp er opprettet for å sikre trygg oppbevaring og tilgangsstyring av sensitive opplysninger. Vi står nå i en situasjon der vi ikke har kontroll over potensiell videre spredning eller bruk av dataene, og det bekymrer oss. Vi oppdaget hendelsen 21.11 kl 23.03 og kontaktet leverandøren klokken allerede 23.14. Vi har foreløpig ikke fått svar.

Konsekvenser

Beskriv mulige konsekvenser avviket har medført for de berørte personene.

• Eksponering av følsomme, fortrolige eller private opplysninger: Informasjon som søknadstekster, arbeidsroller, referanser og personopplysninger (inkludert fødselsnummer) kan ha blitt eksponert på en måte som de berørte personene ikke har gitt samtykke til.
• Potensielt tillitssvikt eller annen betydelig ulempe: For jobbsøkere til stillinger med høyt krav til konfidensialitet, som CISO og sikkerhetsarkitekt, kan det oppstå ulemper som kan påvirke deres profesjonelle omdømme, karriere eller personlige sikkerhet.

Da årsaken til nedlastingen fortsatt ikke er avklart, vil vi komme tilbake med ytterligere informasjon så snart vi har en bedre oversikt.

Tiltak

Beskriv hvilke tiltak som er gjort og planlagt for å forhindre at hendelsen skal skje igjen. Beskriv hva som er gjort for å redusere potensielle skadevirkninger.

1. Revisjon av tilgangsstyring:
• Tilganger til diskområdet er blitt gjennomgått, og tilgangen til leverandøren er slettet.
• Nye retningslinjer for tilgangskontroll og revisjon er under utarbeidelse for å sikre at slike nedlastinger ikke kan utføres uten godkjenning.
2. Tekniske begrensninger:
• Muligheten for manuell nedlasting fra diskområdet vurderes fjernet, slik at tilgang til dokumenter kun skjer via nettbasert visning uten lokal lagring. Vi presiserer at det ikke var mulig å synkronisere filene via feks Google Disk applikasjon, "kun" manuelt laste ned via nettleser. Det utredes om dette nå kan slås av.
• Implementering av logging og varsling i sanntid for mistenkelige aktiviteter, slik at avvik kan oppdages og håndteres raskere. Vi ble varslet, men har nå justert på innstillingene slik at enhver form for nedlasting varsles umiddelbart basert på forbedret regeloppsett.
3. Opplæring og bevisstgjøring:
• Leverandører og ansatte som har tilgang til sensitive opplysninger, vil gjennomgå opplæring i håndtering av data med fokus på personvern og sikkerhet.

Tiltak for å redusere skadevirkninger:
1. Kartlegging av omfang:
• En full gjennomgang av hvilke dokumenter som er lastet ned, er iverksatt for å avklare nøyaktig hvilke opplysninger som kan være berørt.
2. Informasjon til de berørte:
• De berørte personene vil bli informert om hendelsen, inkludert hva slags data som kan ha blitt eksponert, og hvilke tiltak de kan iverksette for å beskytte seg selv.
3. Dialog med leverandøren:
• Leverandøren har blitt kontaktet for å avklare årsaken til hendelsen og for å sikre at dokumentene oppbevares forsvarlig og ikke brukes til uautoriserte formål.
4. Sletting av nedlastede filer:
• Leverandøren vil bli bedt om å bekrefte sletting av alle nedlastede dokumenter og rapportere tilbake når dette er gjennomført.

Informasjon

Har de berørte personene blitt informert om avviket? ○ Ja ◉ Nei

Forklar hvorfor de ikke har blitt informert

Avviket ble oppdaget 23.03 i går, og denne varslingen sendes kl 04.03 påfølgende natt. Vi gjennomgår samtlige filer og involverte nå, og vil varsle de berørte i dag.

22.11.2024 04:10:03 AR644275154

Kontaktinformasjon

Navn og kontaktinformasjon til personvernombud eller kontaktperson hos virksomheten som kan gi mer informasjon om avviket.

Brev fra Datatilsynet vil bli sendt til denne e-postadressen. Oppgi virksomhetens generelle kontaktadresse dersom dette ikke skal sendes direkte til én person.

Navn	Knut Michael Knutsen Haugland
E-post	knut@wayscloud.no
Telefon	91900360
Referanse	

Alternativ kontaktperson

Navn	
E-post	
Telefon	
Referanse	

22.11.2024 04:10:03 AR644275154