[TLP: GREEN]

Beste VCIB, PO,

Analyse situatie Zivver na overname door Kiteworks

Zivver is in juni 2025 overgenomen door het Amerikaanse Kiteworks [1]. Op 13 september publiceerde Follow the Money (FTM) een artikel over deze overname [2]. In de context van discussies over geopolitieke veranderingen, digitale autonomie, digitale soevereiniteit is deze overname het bekijken waard. De IBD en Z-CERT bekeken gezamenlijk de situatie vanuit verschillende perspectieven met als hoofdvraag:

Verandert de overname van Zivver door een Amerikaans bedrijf het risicoprofiel van het gebruik van de Zivver-dienst?

Bij risico's rond informatiebeveiliging en gegevensbescherming kijken we naar beschikbaarheid, vertrouwelijkheid en integriteit. Hierbij is gekeken naar de operationele risico's voor organisaties die de dienst gebruiken. Strategische risico's voor ons land, de Europese Unie en geopolitieke analyses laten we hierbij buiten beschouwing.

Algemeen

Zivver benadrukt dat het technisch landschap niet is veranderd, dat de hosting binnen de Europese Economische Ruimte (E.E.R.) blijft en dat Zivver noch Kiteworks toegang heeft tot via Zivver verstuurde berichten. Wat wel is veranderd is het eigenaarschap van de dienst. Zivver is nu onderdeel van een Amerikaans bedrijf.

Het gebruik van Zivver in de processen en de precieze inrichting van het systeem (on-premise of cloud) verschilt per organisatie, net als het aantal personen of organisaties waarmee via Zivver gecommuniceerd wordt. Elke organisatie moet voor zichzelf beoordelen of de situatie aanleiding geeft om risicoanalyses te herzien. Deze analyse kan hierbij mogelijk helpen.

Beschikbaarheid

De Amerikaanse overheid kan invloed uitoefenen op Amerikaanse bedrijven. Dit risico speelt bij alle diensten waarbij ergens in de keten een eigendomsrelatie met de Verenigde Staten bestaat. Er is daardoor een risico dat de Amerikaanse overheid via Kiteworks de directie van Zivver dwingt om de dienst uit te schakelen (in z'n geheel, voor een gebied of voor een specifieke gebruiker), waardoor de beschikbaarheid in gevaar komt. Vóór de overname door Kiteworks bestond dit risico overigens

ook: Zivver host haar clouddienst weliswaar in de E.E.R., maar wel bij het Amerikaanse Amazon Web Services (AWS).

Voor dit risico geldt dat de impact hoog is en de kans laag maar niet nul gegeven de voorbeelden waarbij het Amerikaanse Microsoft de dienstverlening aan het Internationaal Strafhof wijzigde [3]. Voor Nederlandse gemeenten zijn de risico's rond beschikbaarheid iets toegenomen omdat de Zivver dienst nu direct zou kunnen worden gedwongen om haar diensten te staken.

Vertrouwelijkheid

Voor de opsporing van een strafbaar feit is het onder de Clarifying Lawful Use of Overseas Data Act (CLOUD Act) mogelijk voor Amerikaanse autoriteiten om persoonsgegevens op te vragen bij Amerikaanse cloudproviders, ook als die organisatie de gegevens opslaat buiten Amerika, zoals documenten, foto's en e-mails. Deze wet was al van toepassing door de hosting bij AWS. Zivver stelt zero-access encryptie toe te passen op opgeslagen berichten waardoor personeel van Zivver/Kiteworks (en AWS) geen toegang heeft tot de inhoud van opgeslagen berichten. Bij het gebruik van Data Loss Prevention (DLP) is wel toegang tot de inhoud van de berichten nodig. Dat is een onvermijdelijk onderdeel van het proces. De kernfunctie van een DLP-oplossing is het scannen en monitoren van dataverkeer op basis van vooraf gedefinieerd beleid. Dit beleid bepaalt welke informatie als gevoelig wordt beschouwd, zoals burgerservicenummers, medische informatie of bedrijfsgevoelige gegevens. Ook metadata is anders versleuteld dan de inhoud van berichten. Het FTM-artikel geeft hierop een toelichting. De inrichting van de dienst is niet gewijzigd met de overname.

Risico's rond vertrouwelijkheid zijn in de praktijk ongewijzigd. Er zijn juridisch gezien meer mogelijkheden om data te vorderen, maar bij de inrichting van de dienst is niets gewijzigd. De impact blijft gelijk (maar afhankelijk van hetgeen uitgewisseld wordt via Zivver) en de kans neemt in juridische zin iets toe.

Bekijk de keten

Als we de vertrouwelijkheid van berichtenuitwisseling met Zivver bekijken dan kunnen we niet heen om de stappen voor en na het gebruik. Immers gaat het hier om ongestructureerde datauitwisseling waarbij de verzender gegevens of bestanden verwerkt en die naar de ontvanger stuurt die het op een onbekende plaats opslaat en verder verwerkt.

Het is niet uit te sluiten dat iemand technisch in staat zou zijn om toegang te krijgen tot de inhoud van berichten via Zivver. Statelijke actoren en criminelen hebben hiertoe ongetwijfeld de capaciteiten in huis als de intentie en de belangen maar groot genoeg zijn. De mogelijkheden van detectie zijn beperkt bij dergelijke geavanceerde actoren. Het is evenwel de vraag of een geavanceerde actor geen eenvoudiger middelen tot beschikking heeft om aan informatie te komen. Goed beschouwd kan de informatie ook eerder of later in het proces verkregen worden of door gebruik te maken van niet-technische oplossingen zoals omkoping, afpersing of verleiding.

Integriteit

De factor integriteit van gegevens is nauwelijks van toepassing. De IBD acht de kans en de impact als gevolg van de overname van Zivver door Kiteworks ongewijzigd.

Conclusie

Het gebruik van Zivver in de processen verschilt per organisatie, net als het aantal personen of organisaties waarmee via Zivver gecommuniceerd wordt. Het is aan elke organisatie om te bepalen in hoeverre eventuele gewijzigde inzichten en begrip leiden tot andere risicoafwegingen.

De IBD adviseert gemeenten:

Om te inventariseren waar Zivver voor gebruikt wordt in de organisatie en de risico's daarvan in de gehele keten van verzender naar ontvanger te beschouwen. Om de kwestie rond de overname van Zivver te benutten voor aandacht van management en bestuur voor informatiebeveiliging en gegevensbescherming. De IBD ziet dit als een uitgelezen kans voor de CISO en de PO om het gesprek te voeren over de hoogste risico's voor de organisatie. Om het gesprek over de voornaamste risico's periodiek te houden en dit niet te laten sturen door de waan van de dag. Om een doorlopend een globaal overzicht bij te houden van het applicatielandschap en daarbij te inventariseren wat er per applicatie gebeurt als deze zou uitvallen of als gegevens uitlekken (om welke reden dan ook). Deze inventarisatie geeft een inzicht in het risicoprofiel. Om zo min mogelijk gebruik te maken van ongestructureerde gegevensuitwisseling. E-mail, ook met extra versleuteling, blijft een kwetsbaar medium.

Tot slot willen we het algemene advies benadrukken om risicoafwegingen te herzien wanneer situaties veranderen. Als er wijzigingen optreden in de dienst, dan kan dit aanleiding geven tot nieuwe inzichten en andere maatregelen.

[1] https://www.zivver.com/nl/blog/persbericht-zivver-sluit-zich-aan-bij-kiteworks

[2] https://www.ftm.nl/artikelen/vertrouwelijke-zaken-te-grabbel-na-overname-zivver-door-kiteworks

[3] https://nos.nl/artikel/2567417

Met vriendelijke groet,

VNG Informatiebeveiligingsdienst

Informatiebeveiligingsdienst, Nassaulaan 12, 2514 JS Den Haag