Persbericht – 26 juni 2024

Update gegevensdiefstal

Bijlage: Grondige analyse over gegevensdiefstal afgerond

Randvoorwaarden afgestemd met Vlaamse Toezichtcommissie

De analyse van de gestolen gegevens is complex en neemt tijd in beslag. Er mogen geen bijkomende privacy-risico's genomen worden tijdens de analyse zelf. De oefening moet gebeuren op een veilige, niet-gecompromitteerde dataset, met minimaal datatransport over servers en landsgrenzen heen. Al deze voorwaarden zijn noodzakelijk om de data-analyse op een én juridisch én technisch correcte manier te doen verlopen.
Om die reden wordt voorafgaandelijk een wettelijk verplichte risico-analyse of gegevensbeschermingseffectbeoordeling (ook DPIA, Data Protection Impact Assessment genoemd) uitgevoerd in overleg met De Vlaamse Toezichtcommissie. Deze grondig gedocumenteerde risicoanalyse kon pas worden opgesteld na een diepgaand vooronderzoek en legt de aanpak voor de eigenlijke data-analyse vast.

Voorafgaandelijk onderzoek in vier stappen

1. Na de cyberaanval werd **een duidelijk kader bepaald** dat beschrijft aan welke technische voorwaarden de data-analyse moet voldoen om binnen een veilige context te werken. In deze fase werd ook bepaald op welke dataset de analyse kon plaatsvinden. Op basis van dit kader kon een geschikte datapartner worden aangesteld die binnen een redelijke termijn aan de slag kon. Dit kader werd met de bevoegde overheidsinstanties afgetoetst.

2. Verschillende gespecialiseerde bedrijven werden vervolgens benaderd met de vraag of zij een data-analyse konden uitvoeren binnen het vastgelegde kader, welke methodiek zij hiervoor zouden gebruiken, en binnen welke termijn zij konden beginnen. Gaandeweg werd duidelijk dat de voorgestelde pasklare oplossingen ('**off-the-shelf' technieken**) die een snelle start mogelijk zouden maken, **niet voldeden** aan de vereiste veiligheidsnormen voor deze casus.

3. Hierop volgde een nieuwe zoektocht naar een partner die een **gepersonaliseerde oplossing** kon bieden die aan de nodige voorwaarden zou voldoen. Deze partner werd gevonden in het Belgische bedrijf The Collective. De voorgestelde aanpak werd aan een diepgaande risico-analyse onderworpen en afgetoetst met de bevoegde instanties om er zeker van te zijn dat ze voldeed aan de opgelegde privacy-voorwaarden.

4. Om de veiligheid van gegevens en privacy te waarborgen en ervoor te zorgen dat de gegevensverwerking ook op een wettelijk correcte manier zou gebeuren, volgde een onderzoek waarbij **de voorgestelde aanpak** ook **juridisch-technisch** werd bekeken. Uiteindelijk werd de finale gegevensbeschermingseffect-beoordeling (DPIA) opgesteld, die voorgelegd werd aan de Vlaamse Toezichtcommissie.

Het voorafgaandelijk onderzoek had tot doel om tot deze finale DPIA te komen. Er was voortdurend nauw overleg met de toezichthoudende autoriteiten om zeker te zijn dat de beoogde oplossing(en) zouden voldoen aan de nodige vereisten met als doel geen extra (onverantwoorde) privacy risico's te creëren voor de burgers en onze werknemers. De raad van bestuur werd op geregelde tijdstippen op de hoogte gehouden van de voortgang in dit proces.

Een data-analyse in vier fasen.

Van zodra de DPIA finaal was, konden we van start gaan met de eigenlijke data-analyse. Deze verliep in vier fasen:

1. In de eerste fase vond er een automatische zoekopdracht plaats op metadata op een niet-gecompromitteerde back-up. Deze automatische zoektocht gebeurde anoniem en identificeerde bestanden waarin gevoelige data zouden kunnen zitten op basis van vaste structuren. Voorbeelden van structuren waarop gezocht werd zijn bijvoorbeeld een bankrekeningnummer (bijv. BE11 222 333 444) of een rijksregisternummer (bijv. 00.01.01-123-45).

2. Vervolgens doorzocht een beperkt en intern team bij Limburg.net manueel de gevonden bestanden met de gevoelige gegevens om te weten welke data van welke personen er precies in stonden.

3. Hetzelfde team onderzocht daarna of het om ‘nieuwe’ gegevens ging, dit zijn gegevens waarover Limburg.net eerder nog niet wist dat ze gestolen waren.

4. Over de gegevens waarvan Limburg.net eerder niet wist dat ze gestolen waren, werd aangifte gedaan bij de autoriteiten. Limburg.net informeert ook alle betrokkenen via een persoonlijke brief.

De volledige tijdslijn is terug te vinden via www.limburg.net/persmededelingen.