Persbericht - 29 februari 2024 09:30

Update cyberaanval

Limburg.net stelt cybersecuritymanager aan en informeert gemeenten over extra beveiligingsmaatregelen

Om de gevolgen van de cyberaanval te coördineren stelde Limburg.net eerder deze maand een interim cybersecurity manager aan. Op 27 februari werd hij voorgesteld aan de gemeentelijke DPO's en gaf hij toelichting over de genomen en geplande beveiligingsmaatregelen. Limburg.net streeft naar een maximale openheid rond de cyberaanval en deelt 'lessons learnt' met andere lokale overheden en organisaties.

Cybersecuritymanager aangesteld

Om de technische en juridische trajecten van de cyberaanval te coördineren en aanbevelingen te doen over de verdere versterking van de databeveiliging, stelde Limburg.net een interim cybersecurity manager aan. Algemeen directeur Kris Somers: *We hebben eerder deze maand een cybersecuritymanager aangesteld die ons alvast de komende 6 maanden zal bijstaan in het beheer van de gevolgen van de cyberaanval en om onze databeveiliging verder aan te scherpen. Dit zorgt er ook voor dat onze medewerkers zich verder kunnen focussen op hun operationele kerntaken. Sinds midden februari is EY (Ernst & Young) aan de slag hiervoor bij Limburg.net."*

Hackers forceerden toegang ondanks MFA

Na diepgaande analyse wordt duidelijk hoe de criminelen te werk zijn gegaan. Nadat multifactorauthenticatie (MFA, meervoudige verificatie van de gebruiker) in eerste instantie de aanval kon weren, vonden de hackers een weg naar binnen via een andere toegangspoort waar geen MFA van toepassing op was. Tijdens het tweewekelijks overleg met de DPO's (data protection officers of functionarissen voor gegevensbescherming) van de gemeenten werd dit toegelicht door de cybersecurity manager. Limburg.net deelde ook de technische tijdslijn van de cyberaanval en gaf meer uitleg bij de genomen en geplande beveiligingsstappen en sensibiliseringscampagne.

Zorgvuldige analyse van de gestolen gegevens

De analyse van de gestolen gegevens is complex en moet met de grootste omzichtigheid worden gedaan. De oefening mag geen bijkomende privacy-risico's creëren en moet een duidelijke meerwaarde bieden in de communicatie aan de betrokkenen. Om die reden wordt voorafgaandelijk een 'gegevensbeschermingseffect-beoordeling' (ook DPIA genoemd) opgesteld in overleg met de autoriteiten. In functie van de resultaten van deze 'gegevensbeschermingseffect-beoordeling' zal Limburg.net beslissen welke acties er eventueel volgen. Limburg.net verstuurde al meer dan 270.000 brieven aan de betrokkenen en zal zich blijven inzetten op het correct informeren en sensibiliseren van de inwoners.

Limburg.net zet sensibiliseringsinspanningen voort

Limburg.net blijft zich inspannen om de gevolgen van de cyberaanval aan te pakken. Tegelijkertijd blijft Limburg.net ook gefocust op haar dagelijkse kerntaken. De lopende afvalpreventie-campagnes zullen voortgezet worden, maar er zal ook nadruk blijven liggen op het sensibiliseren over cyberveiligheid. Op 19 januari startte Limburg.net met bewustmaking over de gevaren van identiteitsdiefstal en phishing. Via haar website, sociale media en brieven aan de getroffen inwoners van Limburg en Diest kregen mensen informatie over cybersecurity en tips om zich beter te beveiligen. Limburg.net zal deze boodschap blijven herhalen in de afvalpreventie-communicatie die naar de ruim 381.000 gezinnen in Limburg en Diest wordt verstuurd. Vanaf volgende week krijgt elk gezin een folder met die info in de bus, de boodschap wordt ook herhaald in 'Het Schoonste magazine' en in verdere communicaties.

Perscontact:
Hans Roggen – woordvoerder Limburg.net – 0486 33 90 51
hans.roggen@limburg.net
limburg.net/persmededelingen

Achterkant huis-aan-huisfolder