LOKAAL HENGELO

Aan: College van B&W
Via e-mail: raadsgriffie@hengelo.nl
Datum: 10-11-2022
Betreft: Opensource systemen vormen een levensgrote cyberbedreiging voor de Gemeente Hengelo

Geacht College,

Situatie
De dreiging van digitale aanvallen met o.a. ransomware zijn aan de orde van de dag en nemen toe binnen overheden. De maatschappelijke en financiële schade is vaak niet te overzien. Alleen al immateriële schade is vaak een veelvoud van het IT budget.
Zo ook bij gemeenten in Nederland met Hof van Twente en Buren als recente (bekende) voorbeelden. Hoewel er vaak oorzaak-technisch wordt gekeken naar de organisatie en de menselijke factor is de daadwerkelijke software vaak een blinde vlek in dit soort incidenten.

De informatiebeveiligingsdienst (IBD) van de VNG signaleert, dat er steeds meer en steeds ernstiger fouten in software voorkomen. Deze ernstige fouten in de software die gemeenten gebruiken, aldus de IBD, kunnen worden misbruikt om toegang te krijgen tot systemen.
Een voorbeeld hiervan is het software component Log4J, die er eind 2021 voor zorgde dat tienduizenden software systemen met spoed moesten worden aangepast of worden bijgewerkt. Ook gemeenten moesten die oplossen om incidenten te voorkomen.

Log4J, is zogeheten Open Source Software. Dat is software die vrij beschikbaar is gemaakt voor gebruik. Open Source software wordt juist veel binnen de overheid ingezet om de digitalisering te versnellen en de softwarekosten te verlagen. De zwakke plekken van deze Open Source software is nu net een belangrijke bron van cyberaanvallen.

Volgens Enisa, het Agentschap van de Europese Unie voor cyberbeveiliging, kwamen aanvallen in 2021 voor 66% tot stand via code van derde partijen. Contrast Security schat dat moderne software systemen voor wel 80% uit (open source) code van derde partijen bestaat. Volgens SonaType bevatten tot 30% van de populaire open source pakketten al bekende zwakheden. Door het niet op tijd dichtzetten van deze bekende zwakheden, maken criminelen hiervan gebruik om binnen te komen. Het is immers opensource en alle kwetsbaarheden zijn publiek te vinden. Dus ook door criminelen. **Iedere organisatie binnen de overheid** (bron: AGConnect) **wordt gemiddeld 1.620 keer per week aanvallen**. Dit is een stijging van 44% ten opzichte van het tweede kwartaal van 2021. Van deze organisaties wordt **1 op de 66 wekelijks door ransomware getroffen**.

Waar staan we nu?
Dat een gemeente zelfstandig software bouwt met deze opensource componenten vraagt om disciplinaire huishouding om bekende kwetsbaarheden binnen een paar dagen op te

lossen. De praktijk is echter dat het merendeel van deze kwetsbaarheden pas na 1 jaar worden opgelost. Alle deuren en ramen staan dus letterlijk zo lang open voor iedereen om even een kijkje te nemen of iets ergers uit te voeren. Om zaken nog complexer en onoverzichtelijker te maken gebruiken de meeste open source pakketten op hun beurt weer andere open source pakketten. De afhankelijkheid kan daarmee makkelijk 10 keer groter zijn dan wat direct zichtbaar is. Of anders: je haalt een hoop meer software binnen dan op de verpakking staat. Eigen software maken als gemeente geeft je nog enigszins invloed op de veiligheid, maar leveranciers gebruiken tegenwoordig erg veel Open Source in hun eigen oplossingen. Hoe gaan zij hiermee om?
Volgens de IBD is vaak de ingang voor een cyberaanval ook de software van externe partijen die namens een of meerdere gemeenten diensten uitvoeren.

Stelling
Verouderde opensource systemen vormen een levensgrote cyberbedreiging voor gemeenten en dus ook voor de Gemeente Hengelo.

Vragen:

- Wat is het percentage aan systemen die opensource software bevatten binnen de gemeente Hengelo?
- Wat is het percentage aan systemen die opensource software bevatten binnen de samenwerkingsverbanden en externe leveranciers?
- Hoeveel van deze systemen die opensource componenten bevatten zijn van buitenaf te benaderen, dan wel met het internet verbonden?
- Voldoen deze eigen maatwerk systemen aan de ISO 25010 t.b.v. software veiligheid?
- Voldoen deze systemen van externe partijen en leveranciers aan de ISO 25010 t.b.v. software veiligheid?
    - Zo ja, kan men dit ISO 25010 certificaat overleggen voor ieder specifiek gebruikt systeem?
    - Zo niet, hoe gaat Hengelo dit borgen bij haar eigen maatwerk systemen en die van leveranciers of andere partijen?
- Is er inzicht in de actuele staat (gezondheid) van alle gebruikte open source componenten in het gehele systeemlandschap?
- Heeft de Gemeente Hengelo een IT schadepost gereserveerd n.a.v. een mogelijke cyberaanval?

In afwachting van uw antwoorden.
Glenn Dedecker
Fractie Lokaal Hengelo