

Overzicht ingediende vragen Raad 13 december 2021

	Vragensteller, fractie en onderwerp
1.	Dhr. J.W. Elferink (PVV) – overval woning Euregio - toegelaten
2.	Dhr. V.H.A. van Dijk (D66) – Beperken schade voor gemeente door kwetsbaarheid log4shell in Apache log4j – toegelaten
3.	Dhr. M. Teutelink (BBE) – cybersecurity – toegelaten

1 dhr. J.W. Elferink (PVV) – overval woning Euregio – toegelaten

Het is niemand ontgaan wat er dit weekend en wel op zondag weer gebeurd is in Enschede, een woningoverval op het Euregio terrein, net als 2 weken geleden in Usselo ook een steekpartij met bijna fatale afloop bij de Heurne, een vreselijke mishandeling met een kopschop in Usselo en dan maar te zwijgen over de gebeurtenissen in al de voorgaande maanden met oa de gewelddadige demonstratie van hoofdzakelijk jongeren tussen de 12 en 18 jaar.

De criminaliteit loopt volledig uit de hand hier in onze stad en het is niet veilig, de inwoners hebben zo langzamerhand het gevoel dat de onderwereld, de drugsdealers de messensteker, de overvallers en de kopschoppers, de aanranders en gewelddadige jeugd het in deze stad voor het zeggen hebben, dat kan niet en het mag niet.

Daarom heeft de PVV-Enschede de volgende vragen;

1. Het steeds maar weer uitstellen van het veiligheidsdebat, breed gedragen door de Raad, heeft nog steeds niet plaats gevonden, waarom wordt dit veiligheidsdebat steeds maar weer uitgesteld door de burgemeester vind de burgemeester veiligheid geen issue in onze stad?
2. Is het mogelijk dat de burgemeester zijn invloed in Den Haag kan aanwenden en te zorgen voor meer armslag van politie en de rechtelijke macht om zodoende straffen sneller adequater en zwaarder te kunnen inzetten?
3. Kan de Burgemeester zsm zorgen voor meer inzet van zowel mobiele als vaste camera bewaking?
4. Is er een mogelijkheid om op korte termijn in samenwerking met politie, scholen en ouders een voorlichtingen te organiseren inzake gewelddadige jongeren? Zo jong moeten ze er van doordrongen worden dat we dit als stad en bestuur dit niet accepteren.

2. Dhr. V.H.A. van Dijk (D66) – Beperken schade voor gemeente door kwetsbaarheid log4shell in Apache log4j – toegelaten

Wereldwijd is een ernstige IT-crisis gaande. Op donderdag 9 december is internationaal bekend geworden dat Apache log4j een ernstige kwetsbaarheid bevat, log4shell genoemd. Sinds 2013 zit dit in Java open source code, en dit wordt in allerlei systemen op allerlei computers gebruikt. Naar schatting 3 miljard apparaten bevatten deze kwetsbaarheid. Log4shell zou de grootste en meest kritische kwetsbaarheid van het afgelopen decennium zijn. Problematisch is dat je niet zomaar weet in welke onderdelen van je systeem de kwetsbaarheid daadwerkelijk tot schade kan leiden. Een hacker kan echter eenvoudig achterhalen dát het systeem kwetsbaar is en hier misbruik van maken. Achterdeuren kunnen inmiddels al in systemen geïnstalleerd zijn. Ook al is de kwetsbaarheid in een systeem verholpen, via de

geïnstalleerde achterdeur kunnen kwaadwillenden hele netwerken de komende tijd gaan versleutelen bijvoorbeeld.

D66-raadslid Vic van Dijk heeft zondagavond technische vragen gesteld over de situatie bij de gemeente Enschede en organisaties die gemeentelijke taken uitvoeren. Maandagochtend vroeg kreeg hij al antwoorden (zie hieronder), waarvoor veel dank. Goed dat de gemeente Enschede het weekeinde hard heeft gewerkt om schade te voorkomen. Voor nu de volgende drie vragen voor het college over deze acute situatie:

1. Wil het college in de raadsvergadering de hele raad informeren (mededeling?) wanneer het college op de hoogte was van de ernstige kwetsbaarheid in Apache log4j en wat toen de acties zijn geweest op schade te beperken? De gemeentelijke werkomgeving Citrix is bij NCSC bijvoorbeeld ook in onderzoek.
2. Heeft het college scenario's gemaakt om schade te beperken voor het geval log4shell-achterdeuren al geïnstalleerd zijn, ondanks al het goede snelle werk van de gemeente-ambtenaren? Denk aan de versleuteling van (een deel van) het gemeentelijke netwerk. Of het lekken van data.
3. Wil het college pro-actief de organisaties die gemeentelijke taken uitvoeren tegemoet treden en hulp bieden bij het beperken van schade door log4shell?

<https://en.wikipedia.org/wiki/Log4Shell>

<https://nos.nl/nieuwsuur/artikel/2409121-cyberwaakhond-waarschuwt-voor-gevaarlijk-beveiligingslek>

<https://nos.nl/artikel/2409263-internetwaakhond-deelt-lijst-met-software-die-kwetsbaar-is-voor-hackers>

<https://www.ncsc.nl/actueel/nieuws/2021/december/10/ernstige-kwetsbaarheid-in-apache-log4j>

<https://www.ncsc.nl/actueel/nieuws/2021/december/12/kwetsbare-log4j-applicaties-en-te-nemen-stappen>

<https://www.security.nl/posting/733832/Securitybedrijven+melden+grootschalig+misbruik+Apache+Log4j-kwetsbaarheid>

Een podcast met begrijpelijke uitleg: <https://podcasts.apple.com/us/podcast/stopdebandieten-13-podcast-2-apache-log4j2-log4shell/id1585559038?i=1000544661977>

3. Dhr. M. Teutelink (BBE) – cybersecurity – toegelaten

Er is een ernstige kwetsbaarheid gevonden in Apache Log4j, een Java-log-tool (software bibliotheek) die door veel webapplicaties en -diensten wordt gebruikt. Het Nationaal Cybersecuritycentrum (NCSC) adviseert om de door Apache beschikbaar gestelde updates zo snel mogelijk te installeren / te incorporeren in alle software die gebruik maakt van log4j. Aangezien het een software bibliotheek betreft, en dus geen losstaande applicatie, betekent dit dat er nieuwe versies/releases van bestaande software moeten worden gemaakt en worden geïnstalleerd. De Nederlandse veiligheidswaakhond verwacht op korte termijn misbruik van de kwetsbaarheid die inmiddels de naam Log4shell heeft gekregen. De kwetsbaarheid maakt het voor aanvallers mogelijk de rechten van webserver op afstand te misbruiken. Het NCSC heeft voor deze kwetsbaarheid een High/High-beveiligingsadvies uitgebracht: de kans op misbruik op korte termijn en de potentiële schade zijn groot.

Apache Log4j is breed in gebruik bij grote en kleine organisaties in binnen- en buitenland. De manier waarop deze kwetsbaarheid misbruikt kan worden, is inmiddels publiekelijk bekend. Gezien de vele aandacht voor deze kwetsbaarheid verwacht het NCSC dat de manieren voor misbruik de komende tijd worden doorontwikkeld. Het is daarom extra van belang om de updates snel te installeren.

Burgerbelangen Enschede maakt zich ernstige zorgen over de kwetsbaarheid van de ICT binnen de overheid en heeft daartoe de volgende vragen:

1. is de gemeenten bekend met de genoemde zero-day exploit van log4j en de gevaren die een dergelijke exploit met zich meebrengen?
2. heeft de gemeente inmiddels maatregelen genomen om eigen software aan te passen en heeft de gemeente ook contact met alle software leveranciers over de voortgang tot het patchen van

alle gebruikte systemen? Kan de gemeente garanderen dat deze exploit niet kan worden misbruikt?

3. is er binnen de gemeente een protocol waarmee adequaat kan worden gereageerd op dergelijke zero-day exploits, ook vanuit externe (software) leveranciers? Zo ja, is dit protocol in de ogen van de gemeente toereikend en moet deze worden aangescherpt? Zo nee, is de gemeente voornemens een dergelijk protocol op te stellen en op welke termijn kan deze effectief zijn?