De Woerdense VVD

Mondelinge vragen ex art. 20 RvO

Digitale veiligheid Woerden na Log4j

Twee weken geleden werd een ernstige kwetsbaarheid geconstateerd in Apache Log4j. In de afgelopen dagen zijn ook aanvullende kwetsbaarheden gevonden in nieuw uitgebrachte updates.

Log4j wordt gebruikt in enorm veel applicaties en systemen. Het legt niet alleen de handelingen die computerprogramma's uitvoeren vast, maar probeert ze ook uit te voeren. Door manipulatie van de registraties kunnen hackers Log4j hun eigen, kwaadaardige code laten downloaden en uitvoeren. Zo kunnen ze systemen overnemen, gijzelsoftware installeren of gevoelige data stelen, zo schrijft het NRC.

Daardoor zijn veel organisaties, waaronder gemeenten, kwetsbaar voor misbruik. Het Nationaal Cyber Security Centrum (NCSC) heeft de zwaarste waarschuwing afgegeven: een hoge kans op misbruik met grote schade tot gevolg. Daarom adviseert het NCSC organisaties om zich voor te bereiden op een mogelijke aanval. Verschillende gemeenten en banken hebben hun systemen deels uitgeschakeld in afwachting van reparatie van de kwetsbaarheden. Dat wordt echter flink bemoeilijkt doordat vaak niet duidelijk is welke systemen Log4j allemaal gebruiken.

Daarom heeft de VVD de volgende vragen.

1. Is er zicht op hoeveel systemen binnen de gemeente Woerden en verbonden partijen gebruikmaken van log4j?
2. Welke maatregelen nemen en hebben het college en de organisatie genomen om de kwetsbaarheid te verhelpen en aanvallen tegen te gaan, voor zover in de openbaarheid valt toe te lichten?
3. Hoe bereidt het college zich voor op mogelijk misbruik, voor zover in de openbaarheid valt toe te lichten?
4. Is het college bereid om de raad op een later moment uitgebreider te informeren over de digitale veiligheid van de gemeente Woerden?

Namens De Woerdense VVD,

Florian van Hout