Beantwoording vragen rondom kwetsbaarheid Apache Log4j

Vragen van dhr. van Dijk en dhr. Teutelink

Graag dienen Marc Teutelink en Vic van Dijk de volgende rondvraag voor de raadsvergadering vanavond in:

Naar aanleiding van de rondvragen van BBE en D66 vorige week maandag 13 december 2021 over de kwetsbaarheid log4shell stuurde de wethouder op vrijdagavond 17 december meer informatie naar de gemeenteraad. Hieruit bleek dat de VMWare thuiswerkomgeving die avond is uitgeschakeld op basis van “de laatste informatie van de IBD/NCSC.” BBE en D66 stellen daarom de volgende rondvraag aan het college van burgemeester en wethouders van Enschede:

1. **Wanneer ontving het college de informatie over de kwetsbaarheid van VMWare als gevolg van log4shell? Op 10 december 2021 was immers al duidelijk dat VMWare kwetsbaar kon zijn, zie [1,2]. Inmiddels is ook duidelijk dat de Russische criminele groep Conti ransomware-aanvallen uitvoert op VMWare servers. [3]**

   Beantwoording:
   - Zoals vorige week maandag aangegeven is het college maandag 13 december 2021 geïnformeerd over de kwetsbaarheid in Log4j.
   - Op vrijdag 10 december 2021 werd door VMware onderzocht in hoeverre haar producten gevoelig zijn voor de Log4j kwetsbaarheid en gaven op de website aan dat het “under investigation” was. Daarmee was op vrijdag 10 december 2021 nog niet duidelijk dat de producten van VMWare daadwerkelijk kwetsbaar zouden zijn.
   - Op zaterdag 11 december 2021 werd bekend dat de producten van VMware kwetsbaar zijn. De door de leverancier beschreven workarounds zijn door onze IT-medewerkers op zaterdag 11 december 2021 toegepast. De kwetsbaarheid was (met de informatie die toen voor handen was) weggenomen.
   - Op vrijdag 17 december werd duidelijk dat een nieuwe kwetsbaarheid van Log4j hoger werd ingeschaald. Aangezien voor het thuiswerkportaal van VMware, op dat moment geen patch of workaround beschikbaar was, hebben we besloten om dit uit te schakelen.
   - Op zondag 19 december 2021 is onze VMware omgeving bijgewerkt en daarmee is deze kwetsbaarheid weggenomen.

2. **Eerdere antwoorden van het college suggereren dat draaiboeken en scenario’s voor het geval (een deel van) het gemeentelijke netwerk versleuteld raakt niet bestaan. Wil het college die nu als de wiedeweerga opstellen voor het scenario van versleuteling door kwaadwillenden? Wat als door de kwetsbaarheid in VMWare, of een ander onderdeel, de gemeente te maken krijgt met ongewenste versleuteling?**

   Beantwoording:
   In het geval dat (een deel van) het gemeentelijke netwerk versleuteld raakt dan zijn wij daarop voorbereid. Vanuit het vigerende crisisprotocol leggen wij meteen contact met onze externe partner. Hiermee is een Incident Response Retainer afgesloten wat inhoudt dat in geval van een hack er binnen een x-aantal uur een team van specialisten op locatie is om de bedreiging te minimaliseren, forensisch bewijs veilig te stellen en samen te komen tot een herstelplan en wederopbouw. Het draaiboek en/of protocol van de retainer is dan leidend. Deze hebben wij zelf niet in ons bezit.

   Daarnaast hebben we met een externe gespecialiseerde partner de Managed Detection & Response ingericht. Dit houdt in dat 24x7 onze omgeving wordt gemonitord op verdachte activiteiten of kwetsbaarheden. Zo nodig schakelt de externe partij met het IT Bedrijf om gerichte maatregelen te treffen.

3. **Het lijkt erop dat het college achter de feiten aan loopt. Wil het college daarom experts van buiten betrekken om zo een “second opinion” te krijgen en de aanpak van de log4shell-crisis te verbeteren?**

Beantwoording:
Bij onze aanpak zijn verschillende experts betrokken zoals de Informatiebeveiligingsdienst, beveiligingsexperts en verschillende leveranciers. Zo adviseert onze Managed Detection & Response dienstverlener ons bij de te nemen maatregelen. Daarnaast helpt onze VMware implementatiepartner bij de te treffen maatregelen rondom de VMWare producten.
We zijn met man en macht deze kwetsbaarheid aan het managen.
Een second opinion is naar onze mening op dit moment niet noodzakelijk. Wij gaan vanzelfsprekend evalueren waarbij we ook onze expert partners betrekken.

***