College

Raadsinformatiebrief

Aan	Raad
Portefeuillehouder	Mark van Stappershoef
Onderwerp	Beveiligingsincident Log4j
Datum	21-12-2021

Wat is er aan de hand?
Vrijdagmiddag 10 december is er een wereldwijde kwetsbaarheid (log4j) ontdekt, waarop het Nationaal Cybersecurity Centrum (NCSC) en de Informatiebeveiligingsdienst (IBD) alarm sloegen. De kwetsbaarheid zit ingebakken in veel software. Daarom raakt dit wereldwijd vele bedrijven en organisaties. Leveranciers van software zijn sinds vrijdag bezig om in de eerste plaats te onderzoeken of zij deze kwetsbaarheid aantreffen, en zo ja, om updates voor hun software uit te brengen.

Wat is het risico?
Via deze kwetsbaarheid kunnen kwaadwillende zich toegang verschaffen tot het netwerk. Daarmee kunnen zij bijvoorbeeld (persoons)gegevens buitmaken of ransomware (gijzelingssoftware) installeren.

Wat is er gedaan?
Na ontvangst van de melding van de IBD is Equalit samen met de CISO's van de gemeenten direct gestart met het onderzoek naar de impact. Equalit volgt daarbij het handelingsperspectief van de IBD. Uit voorzorg zijn direct een aantal servers uitgeschakeld. De impact daarvan is voornamelijk intern en de dienstverlening is niet in gevaar geweest. Daarnaast is gestart met het benaderen van leveranciers om na te gaan of zij risico lopen en of een oplossing beschikbaar is om de kwetsbaarheid weg te nemen.

Zijn we veilig?
Dat kunnen we niet met zekerheid zeggen. De dreiging van de log4j kwetsbaarheid is nog niet weggenomen. Wij hebben een korte lijn met de IBD en Equalit heeft permanent verhoogde dijkbewaking ingeschakeld om ons netwerk te beschermen. Voor zover we weten is er tot op dit moment geen misbruik gemaakt van de log4j-kwetsbaarheid op de systemen. Risicovolle systemen worden pas weer vrijgegeven, wanneer de leverancier de kwetsbaarheid heeft verholpen. Daarnaast focussen we ook op applicaties die niet door Equalit gehost worden (zogenoemde SaaS applicaties). Voor deze leveranciers gelden dezelfde uitgangspunten.

Hoe verder?
De komende dagen, naar verwachting zelfs weken, zal nog veel aandacht moeten worden besteed aan het onder controle krijgen van de log4j-kwetsbaarheid. Dit gebeurt door het direct plaatsen van alle benodigde updates die leveranciers aanbieden. Equalit blijft daarbij continu het netwerk monitoren. Als er risico's optreden, worden direct maatregelen getroffen. Het kan voorkomen, dat daarbij bedrijfskritische applicaties worden gestopt. Hiertoe zal alleen worden besloten als het risico zo hoog is, dat snelheid de voorkeur geniet, om erger te voorkomen. Daarover zal bestuur, directie en management direct worden geïnformeerd. Er is tot nu toe, door de genomen maatregelen, geen aanleiding geweest om bedrijfskritische applicaties te stoppen.

Het scenario "wij blijven open" is afgestemd en in lijn met wat de G5, B5 en de Veiligheidsregio doen. Daarnaast is aandacht voor als het misgaat. Voor de kerstperiode worden noodscenario's ingericht voor als een bedrijfskritische applicatie toch uit voorzorg moet worden uitgezet, of erger – als misbruik leidt tot een geslaagde inbreuk en er op grotere schaal systemen plat gaan.

https://nos.nl/artikel/2409383-stilte-voor-de-storm-door-groot-beveiligingsprobleem-dit-gaat-niet-met-een-sisser-aflopen