gemeente opmeer

RAADSINFORMATIEBRIEF

Postregistratienummer	21.0016992

Opmeer, d.d.: 22 december 2021

Onderwerp

Raadsinformatiebrief over: Cyber Security

Aanleiding

Op donderdag 9 december is er een nieuwe kwetsbaarheid geconstateerd binnen de Apache Log4J software. Deze software wordt wereldwijd gebruikt in logging tools (vastlegging van handelen door mens en systeem). Deze software zit veelal 'ingebakken' in software pakketten en in 'firmware' voor het aansturen van hardware. Daarnaast is het slecht te detecteren. Men ziet de Apache Log4J software niet staan in de softwarelijst op een computer en hierdoor is men veelal niet bewust dat dit aanwezig is op de eigen systemen.
De kwetsbaarheid betreft het kunnen binnen komen in systemen en daar allerlei handelingen kunnen uitvoeren. Via allerlei mogelijkheden waarmee computers met elkaar in verbinding staan kan een netwerk of netwerken op deze wijze worden ondermijnd (bv. stelen van data, ransomeware plaatsen of regie in netwerk overnemen).

Maatregelen

De Informatiebeveiligingsdienst (IBD), in samenspraak met het Nationaal Cyber Security Center (NCSC), heeft overheden op vrijdag 10 december op de hoogte gesteld van deze kwetsbaarheid. Door het wereldwijde voorkomen op brede schaal en de ernst van de kwetsbaarheid is direct opgeschaald tot een melding met zeer hoge urgentie/impact.
SSC DeSom heeft daarop direct geïnventariseerd (middels specifieke tools) of deze software ook binnen ons gehele netwerk voor komt. Dit bleek inderdaad het geval. Daarop zijn direct patches en fixes (oplossingen voor dit probleem) vanuit de leverancier geïnstalleerd. Echter, dit kan alleen binnen de eigen beheerde systemen. SSC DeSom en onze gemeente zijn sterk afhankelijk van veel software-leveranciers.
Vanaf zaterdag 11 december kwamen de eerste berichten binnen vanuit software-leveranciers over hun inventarisatie en de eventuele maatregelen welke zij genomen hadden. Leveranciers van onze kern-applicaties hebben maatregelen genomen en hebben hiervoor updates, patches en/of fixes uitgebracht.
Ook is informatie binnen gekomen dat bepaalde update en fixes weer andere kwetsbaarheden met zich meebrachten, waardoor systemen continue voorzien moeten worden van deze updates. SSC DeSom heeft meerdere malen, middels digitaal forensisch onderzoek, geconstateerd dat we nog niet geraakt zijn.

GBT

Op woensdagavond 15 december zijn, op basis van het advies vanuit SSC DeSom en de gemeentelijke CISO's (Chief Information Security Officer) om aanvullende maatregelen te nemen om het risico op inbreuk sterk te verminderen, de bestuurders van alle regio-gemeenten geïnformeerd. In dit overleg is besloten tot het installeren van een GBT (Gemeentelijke Beleid Team). Dit team bestaat uit bestuurders van de regio-gemeenten, directeur en CISO van SSC DeSom, gemeentelijke communicatie-adviseurs en CISO's. Doel is om deze kwetsbaarheid en de genomen maatregelen te bespreken en bij eventueel verhoging van het dreigingsniveau aanvullende maatregelen snel te kunnen nemen. Tevens kan op éénduidige wijze communicatie richting medewerkers, inwoners, bedrijven, ketenpartners en andere betrokkenen plaats vinden. Het GBT komt één maal per dag (digitaal) bij elkaar. Bij verhoogde dreiging zal dit worden opgeschaald.

Huidige impact

De huidige maatregelen hebben geen beperkingen op de dienstverlening richting onze inwoners en bedrijven. Ook onze ketenpartners ondervinden geen hinder van deze restricties. Echter, het valt niet uit te sluiten dat in de komende dagen nog aanvullende maatregelen moeten worden genomen welke wel effect zullen hebben op de dienstverlening. Indien dit van toepassing is zullen we dit uiteraard goed communiceren naar inwoners en bedrijven via de standaard communicatiekanalen.

Vervolg

Hoewel er tot nu veel werkzaamheden zijn verricht door SSC DeSom, gemeenten en leveranciers is deze kwetsbaarheid nog niet onder controle. Enerzijds omdat kwaadwillende via deze (of nieuwe) kwetsbaarheid aanvallen blijven ondernemen en anderzijds omdat deze software wereldwijd geïnstalleerd is en door onbekendheid met de materie veelal kleine ondernemingen met beperkte ICT capaciteit geen goede beoordeling kunnen maken. Hierdoor bestaat een grote kans dat 'het vuur niet geblust kan worden en telkens opnieuw oplaait'.
Waakzaamheid is zeker de komende weken, zo niet maanden, geboden, waarbij snel gereageerd dient te worden op nieuwe aanvallen vanuit deze bestaande kwetsbaarheid. SSC DeSom en de gemeentelijke CISO's zijn zich terdege bewust van de risico's en blijven de informatie van IBD en NCSC op de voet volgen.

Hoogachtend,

M.A.S. Winder
Gemeentesecretaris

G.J. van den Hengel
Burgemeester

Wij werken op afspraak
Hebt u een product of dienst nodig van de gemeente? Maak een afspraak via www.opmeer.nl