Algemene informatiebrief 3:

Informatie ten behoeve van besturen en raden.

Inleiding

In navolging van de informatie die wij op 23 december jl. aan u hebben verstrekt, ontvangt u hierbij op de rand van 2021 de laatste stand van zaken over de kwetsbaarheid in Log4j.

Aanleiding

Vrijdag 10 december jongstleden zijn we door de IBD geïnformeerd over een ernstige kwetsbaarheid in Apache Log4j. Deze software komt wereldwijd in heel veel systemen voor, ook bij gemeenten. Log4j vindt men terug van kernapplicaties als Key2Burgerzaken tot in webformulieren met een invulveld. Gezien de omvang van de mogelijke kwetsbaarheden en het gemak waarmee hackers hier gebruik van kunnen maken, is de situatie door de IBD en NCSC aangemerkt als het grootste risico van de afgelopen 10 jaar. Deze informatie is adequaat opgepakt en er is direct begonnen met inzet op het verminderen van de kwetsbaarheid.

Verminderen kwetsbaarheid op meerdere niveaus

- Om de risico's in kaart te kunnen brengen en de zoekrichting te versmallen is en wordt de omgeving door 3 verschillende partijen (KPN, IBD en de RID) gescand op mogelijke kwetsbaarheden. Door de RID is een professioneel pakket aangeschaft waarmee op dagelijks niveau regionaal gescand wordt. De informatie uit al deze scans geeft een zoekrichting naar mogelijke vermindering van de kwetsbaarheden. Inmiddels zijn bevindingen uit deze scans die vroegen om actie met een hoge prioriteit opgepakt. In een samenwerking tussen de ICT-regisseurs, functioneel applicatiebeheer (hierna FAB) en de RID zijn de benodigde mitigerende maatregelen genomen.
- Er wordt niet louter vertrouwd op bovengenoemde techniek. Naast de scans, wordt daarom ook ingezet op blijvende alertheid van de betreffende medewerkers zelf.
- Parallel is in uw organisaties en bij de RID gewerkt aan het vergaren van benodigde informatie. Het gaat hierbij om servers, bijna 800 applicaties (waarvan een deel in de cloud met een koppeling naar systemen) en een onbekend aantal websites. Uit de inventarisatie is gebleken dat veel hiervan niet (volledig) in beeld was bij onze organisaties en daarmee ook niet bij de RID. Voor informatie over applicaties zijn we bovendien meestal afhankelijk van leveranciers.
- Alle vergaarde informatie vanuit de organisaties, leveranciers en de RID, wordt gebundeld op één overzichtslijst waar alle mutaties moeten worden verwerkt.
- Naast de inventarisatie (kwantitatief) wordt nagegaan of de bewuste Log4j bouwsteen aanwezig is en is begonnen, met behulp van de beslisboom van de IBD, met de afweging of overgegaan moet worden tot aanpassen, updaten of uitzetten (kwalitatief). Prioritering van de acties vindt op dagelijkse basis plaats en wordt mede bepaald door de bevindingen die uit de scans komen.
- In het kader van algemene informatiebeveiliging is de harde realiteit dat kwetsbaarheid (los van Log4j) voor een belangrijk deel nog steeds wordt veroorzaakt door makkelijk te hacken wachtwoorden van gebruikers. Deze blijven daarmee een te groot risico vormen voor de informatiebeveiliging. Versnellen van de implementatie van sterke wachtwoorden per 1 februari '22, conform authenticatiebeleid, vermindert deze kwetsbaarheid.

Mogelijk misbruik in de kerstvakantie

Onder normale omstandigheden is de kerstvakantie altijd al een kwetsbare periode door de lagere bezetting. Daar komt dus dit jaar door Log4j nog een extra risico bij. De verwachting is dat het misbruik vooral gericht is op financieel gewin door ransomware. Ook kunnen criminelen toegang verkrijgen tot de systemen en deze toegang pas over een paar maanden gebruiken voor een gerichte ransomware aanval. Vanuit de keteneffecten kan verstoring tot een domino-effect leiden. Door de IBD wordt bovenstaande aangemerkt als een reëel scenario.
Het gegeven dat er tijdens de kerstdagen geen verdachte activiteiten zijn waargenomen, geeft daarom geen garanties op veiligheid. De inzet blijft daarmee volledig gericht op het verminderen van de kwetsbaarheden.

Extra inzet vanuit de organisaties

Deze en komende weken wordt daarom structureel ingezet op verhoogde 'dijkbewaking'. De RID heeft bereikbaarheid en beschikbaarheid geborgd in voorbereiding op de noodzakelijke patches, updates en andere mitigerende maatregelen. En ook bij uw organisaties is voor de komende weken zowel bij de ICT-regisseurs als de FAB-ers stevig ingezet op extra capaciteit, allereerst op de kritische bedrijfsapplicaties of hoge prioriteiten door bevindingen uit de scans. Tenslotte is voor het beheren en onderhouden van de overzichtslijst extra inzet geregeld.

Extra opbrengsten vanuit dagelijkse scan

De RID heeft zoals aangegeven een professioneel pakket aangeschaft waarmee een dagelijkse scan op kwetsbaarheden wordt uitgevoerd. Net als een MRI levert zo'n goede scan altijd veel meer en specifiekere informatie op. Naast de bevindingen over Log4j, heeft deze scan dus ook resultaten opgeleverd over andere kwetsbaarheden. Alles onder een afgesproken risiconorm valt onder regulier patchbeleid, alles daarboven vraagt door de hogere prioriteit om een andere benadering. Ook voor de extra bevindingen moeten dus de risico's in kaart gebracht worden. Deze werkzaamheden moeten bovenop de nog honderden kleinere kwetsbaarheden op het gebied van Log4j worden opgepakt door dezelfde groep medewerkers; de ICT-regisseurs, FAB en de RID. Ook dit heeft consequenties voor de beschikbaarheid en dienstverlening vanuit deze medewerkers op de langere termijn. Daarom worden tevens de effecten op de gewenste werkzaamheden voor 2022 vanuit de actielijst Informatiebeveiliging in kaart gebracht.

Dringend advies aan iedereen: let op je wachtwoorden

Ook de komende periode blijft het dringende advies aan iedereen om alle apparaten en apps (zakelijk én privé) zo vaak mogelijk te updaten, geen nieuwe privé-apps op zakelijke apparaten te downloaden en niet op verdachte linkjes in de mail te klikken.
Gezien de nieuwe bevindingen uit de scans raden we daarnaast met klem aan om eens goed naar uw eigen wachtwoorden te kijken. Zijn ze lastig te hacken of nog steeds te makkelijk? In teveel gevallen blijft dit één van de meest kwetsbare onderdelen.

Meer informatie

We houden u op de hoogte van de stand van zaken. Mocht de situatie daarom vragen, informeren wij u uiteraard tussendoor.