Kwetsbaarheden in Citrix: Lessen voor gemeenten en de IBD

In december 2019 werden kwetsbaarheden in de Citrix-producten Citrix ADC en Citrix Gateway servers (voorheen Netscaler) bekend. Deze kwetsbaarheden bleken uiteindelijk zo ernstig dat landelijk door het NCSC het advies werd uitgevaardigd om deze systemen uit te zetten tot een volledige oplossing beschikbaar was. Vanwege de impact die dit heeft gehad op de bedrijfsvoering van gemeenten en mogelijk vergelijkbare incidenten in de toekomst is gekozen om de lessen uit deze kwestie op te tekenen in deze factsheet.

Inleiding

Hard- en software, nieuw of al bestaand, bevatten fouten en kwetsbaarheden. Fouten en kwetsbaarheden kunnen worden misbruikt door kwaadwillenden. De kans dat dit daadwerkelijk gebeurt en de impact als dat gebeurt verschillen per geval. Wanneer in een product een kwetsbaarheid wordt ontdekt dan volgt in de regel een oplossing van de fabrikant. Communicatie over de kwetsbaarheid en de oplossing van de fabrikant gaan dan hand in hand. Op basis van een risico inschatting (kans x impact) is dan van de gebruiker actie vereist. In 2019 alleen verzond de Informatiebeveiligingsdienst (IBD) 1751 waarschuwingen over kwetsbaarheden, waarvan 23 met een hoge kans op misbruik en een hoge impact (h/h).[1] Een van die h/h-kwetsbaarheden was er een in Citrix ADC en Gateway. Bijzonder in deze situatie was dat de kwetsbaarheid bekend werd terwijl nog geen volledige oplossing vanuit de fabrikant beschikbaar was.

Scans door de IBD

Begin januari kwamen instrumenten om te scannen en misbruik te maken van de kwetsbaarheid[2] publiekelijk beschikbaar. De IBD heeft hierop alle, bij de IBD bekende, IP-adressen van gemeenten gescand op aanwezigheid van de kwetsbaarheid. Een aantal gemeenten bleek op 13 januari nog niet alle geadviseerde mitigerende maatregelen te hebben doorgevoerd. Gemeenten die op dat moment nog kwetsbaar waren zijn gebeld en de IBD heeft deze gemeenten geadviseerd over de maatregelen en hen begeleid in de analyse van logbestanden om te zien of misbruik is gemaakt. Het percentage misbruik van kwetsbare systemen bleek zeer hoog en dit beeld strookte met analyses[3] van beveiligingsonderzoekers.[4]

Advies NCSC en IBD

Op 16 januari vaardigde het NCSC (mede op basis van een bericht van de AIVD) het advies uit om Citrix-systemen uit te schakelen waar dat kon en anders aanvullende maatregelen te treffen.[5] Vanuit leveranciers kwamen tegenstrijdige berichten, zo achtte Fox-IT het niet nodig om Citrix uit te schakelen.[6] De IBD heeft in afstemming met het NCSC het advies om Citrix ADC en Gateway uit te schakelen tenzij dat echt niet anders kan ook voor gemeenten uitgevaardigd. Dit ondanks het feit dat we ons hierbij moesten baseren op zeer beperkte en soms tegenstrijdige informatie. Het hoge percentage misbruik en de eenvoud waarmee het misbruik kon plaatsvinden gaf uiteindelijk voldoende reden om het zware advies voor gemeenten over te nemen.

Communicatie naar alle gemeenten o.a. via SMS

Vanwege de aard en de ernst van de adviezen en omdat de IBD niet van alle gemeenten beschikt over een actuele ICT-foto of een volledig overzicht van IP-adressen besloot de IBD de adviezen naar alle gemeenten te versturen. Omdat in sommige gemeenten e-mail niet meer beschikbaar was hebben we alle adviezen in verkorte vorm ook per SMS naar onze contactpersonen verstuurd.

Opvolging door gemeenten

Veel gemeenten besloten daarop Citrix-systemen uit te schakelen. Dit had consequenties voor het werk van de gemeenteambtenaren: thuiswerken was in veel gevallen niet meer mogelijk, dienstverlening op afstand kon niet op de normale wijze doorgaan en in sommige gevallen lag het e-mailverkeer stil. Er waren ook gemeenten die op basis van een risicoafweging welbewust de keuze maakten om Citrix aan te laten staan in combinatie met extra maatregelen zoals verscherpte monitoring en detectie. Ook bleken gemeenten zonder Citrix toch last te hebben van de maatregel om Citrix uit te zetten, bijvoorbeeld omdat leveranciers of ketenpartners gebruik maakten van Citrix voor bijvoorbeeld clouddiensten.

Wat had er mis kunnen gaan

Organisaties die na het verschijnen van de scan tools en de exploits(de op internet beschikbare instrumenten om misbruik te maken van de kwetsbaarheden), geen mitigerende maatregelen hebben doorgevoerd moeten er rekening mee houden dat onrechtmatige toegang is verkregen tot de systemen. Toegang is een van de eerste voorwaarden voor verdere actie van een crimineel of statelijke actor. De volgende stap[7] is dat verder wordt verkend wat de mogelijkheden zijn. Het is bekend dat daders hier lang en uitgebreid de tijd voor nemen. De dader kan uiteindelijk toegang krijgen tot vertrouwelijke informatie, informatie wijzigen, vernietigen of systemen uitschakelen. Een beproefd bedrijfsmodel van criminelen is het versleutelen van bestanden om deze in ruil voor losgeld weer vrij te geven, de zogenaamde ransomware. De gevolgen voor gemeenten zouden desastreus zijn: zeker wanneer de criminelen ook alle back-ups onklaar hebben gemaakt. Recente voorbeelden na ongepatchte kwetsbaarheden[8] van o.a. het grenswisselkantoor GWK Travelex,[9] de universiteit van Maastricht[10] en verschillende Amerikaanse gemeenten[11] laten zien dat dit risico zich werkelijk manifesteert. Ook zonder geslaagde aanval kunnen de kosten ver oplopen, door bijvoorbeeld forensisch onderzoek, onderbreking van werkzaamheden of kosten om systemen opnieuw in te richten.

Observaties van de IBD

- **Niet alle gemeenten hadden de mitigerende maatregelen doorgevoerd ondanks de vele waarschuwingen vanuit de IBD en de CISO**. Opvallend was dat CISO's van een aantal gemeenten dachten dat de maatregelen wel waren doorgevoerd. Navraag leerde dat de urgentie van de adviezen van de CISO niet helder was en dat soms niet alle systemen in beeld waren.
- **Gemeenten hebben niet alle systemen in beeld.** Gemeenten hebben niet altijd een volledig overzicht tot op versieniveau van hetgeen in hun ICT-omgeving aanwezig is. Overzichten worden wel gemaakt, maar bijhouden is doorlopend werk.
- **Niet alle afhankelijkheden zijn in beeld.** Het is niet altijd helder welke processen afhankelijk zijn van welke systemen. Extra aandacht blijkt nodig voor clouddiensten waarbij leveranciers gebruik maken van systemen die kwetsbaarheden kunnen bevatten.
- **In de communicatie vanuit VNG / IBD ontbreekt een snelle en directe lijn naar bestuurders.** De IBD kan snel schakelen met ACIB's en VCIB's van gemeenten. Bij Citrix bleek een behoefte om bestuurders van gemeenten te informeren over de afwegingen die in afstemming met het Rijk zijn gemaakt en de afwegingen die op lokaal niveau nog gemaakt dienden te worden. De VNG/ IBD verkent de mogelijkheden om een proces in te richten voor dergelijke communicatie.

Adviezen aan gemeenten

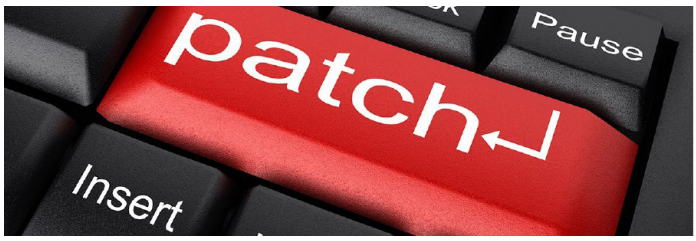
- **Integreer het crisismanagementproces voor informatiebeveiliging in de reguliere crisisstructuur en oefen dit regelmatig.** Het is van het hoogste belang dat voor informatiebeveiligingsincidenten een eenduidige opschalingsstructuur bestaat in de gemeente of het samenwerkingsverband. In elk geval zit in een dergelijk proces de bestuurder aan tafel met de CISO als eerste adviseur, de relevante afdelingsmanagers, communicatie / woordvoering en ICT. Geef de CISO het mandaat om in gevallen van acute incidenten dwingende adviezen uit te vaardigen terwijl de opschaling plaatsvindt. Bijvoorbeeld zoals het hoofd BHV mag besluiten tot een ontruiming.[12]
- **Maak werk van de basismaatregelen en -processen.** Voorkomen is beter dan genezen. Zeker bij informatiebeveiliging. Een organisatie met de basismaatregelen en -processen op orde (weten wat je in huis hebt, dat up-to-date houden en zorgen dat medewerkers veilig hun werk kunnen doen) kan de risico's op een geslaagde digitale aanval tot acceptabele niveaus reduceren. Anders gezegd: zonder deze basismaatregelen zijn organisaties weerloos tegen criminelen. Een ding is zeker: de kosten van incidentmanagement, forensisch onderzoek en herstel na een incident zijn vele malen hoger dan de kosten van juist ingerichte basismaatregelen en -processen.
- **Actualiseer de bedrijfscontinuïteitsplannen voor uitval van kritieke ICT-componenten.** Inventariseer per afdeling de kritieke processen en ga na welke ICT-componenten essentieel zijn voor de uitvoering daarvan. Maak voor gehele of gedeeltelijke uitval van die componenten een plan en bepaal in welke mate uitval acceptabel is. Ten slotte is het van belang om de kritieke processen voor de organisatie als geheel te prioriteren. De IBD inventariseert of het mogelijk is om in dit kader samen met gemeenten een format te maken voor een prioritering van gemeentelijke processen.

Verhogen digitale weerbaarheid

Via VNG en IBD zijn diverse games en daadwerkelijke oefeningen beschikbaar die u specifiek op lokaal niveau helpen om binnen uw gemeente inzicht te krijgen in de consequenties van dit type incidenten en stellen u in staat daarmee daadwerkelijk te oefenen.[13] De IBD werkt met een gericht programma aan de structurele verhoging van de digitale weerbaarheid van gemeenten in lijn met de Agenda Digitale Veiligheid van VNG.[14] Vanaf 2020 intensiveren we deze aanpak met losse modules voor de belangrijkste maatregelen en processen. Met behulp van webinars, (technische) workshops, best practices en concrete hulpmiddelen kunnen gemeenten aanhaken op de gebieden waar verbetering nodig is. Er wordt in eerste instantie aan de slag gegaan met het verbeteren en optimaliseren van configuratiebeheer. Tegelijkertijd loopt een pilot netwerkinventarisatie (NWI).[15] Deze pilot is bedoeld om te zien of het mogelijk is om geautomatiseerd de gemeentelijk ICT-overzichten actueel te krijgen en te houden. Zo kan namelijk een verbetering gerealiseerd worden op configuratie- en patchmanagement.

Vragen of opmerkingen?

Heeft u naar aanleiding van deze factsheet vragen of opmerkingen? Neem dan contact op met de IBD via 070 – 204 55 11 of info@IBDGemeenten.



Meer informatie

Meer informatie over onze dienstverlening vindt u in de andere factsheets van de IBD en op de website www.informatiebeveiligingsdienst.nl. De helpdesk van de IBD is te bereiken tijdens kantooruren van 9:00 tot 17:00 uur op het nummer 070 204 55 11 of via het e-mailadres info@IBDgemeenten.nl. De CERT van de IBD is 24x7 bereikbaar via 070 204 55 11 (instructies voor het piketnummer op de voicemail).

Links in dit document

1 https://www.informatiebeveiligingsdienst.nl/nieuws/ibd-jaaroverzicht-2019/
2 https://isc.sans.edu/forums/diary/Citrix+ADC+Exploits+are+Public+and+Heavily+Used+Attempts+to+Install+Backdoor/25700/
3 https://www.bleepingcomputer.com/news/security/ragnarok-ransomware-targets-citrix-adc-disables-windows-defender/
4 https://www.fireeye.com/blog/products-and-services/2020/01/fireeye-and-citrix-tool-scans-for-iocs-related-to-vulnerability.html
5 https://www.ncsc.nl/actueel/nieuws/2020/januari/16/door-citrix-geadviseerde-mitigerende-maatregelen-niet-altijd-effectief
6 https://resources.fox-it.com/rs/170-CAK-271/images/20200118_Citrix_advisory_UPDATE_1.pdf
7 https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
8 Deze voorbeelden zijn hoogstwaarschijnlijk het gevolg van kwetsbaarheden in andere systemen dan Citrix
9 https://www.computerweekly.com/news/252476283/Cyber-gangsters-demand-payment-from-Travelex-after-Sodinokibi-attack
10 https://www.maastrichtuniversity.nl/nl/faq-cyberaanval-um
11 https://en.wikipedia.org/wiki/2019_Baltimore_ransomware_attack
12 Zie ook de Agenda Digitale Veiligheid 2020-2024 van VNG: https://www.informatiebeveiligingsdienst.nl/nieuws/agenda-digitale-veiligheid-biedt-perspectief/
13 https://www.vngacademie.nl/Training/train-de-trainer-vng-cybergame/9f90ae2f-8a8d-4305-9047-1d69f4b68aa7
14 https://www.informatiebeveiligingsdienst.nl/project/digitaleweerbaarheid/
15 https://www.informatiebeveiligingsdienst.nl/nieuws/pilot-netwerkinventarisatie-nwi-pilot-gestart/