Systeembeheerders in de zorg: Wakker worden! Enorme kwetsbaarheid in Citrix Application Delivery Controller

Vanaf half december 2019 is bekend dat er een forse kwetsbaarheid zit in de software van een aantal apparaten van de firma Citrix. Het gaat om de Citrix Application Delivery Controller (ADC). Die stond eerder bekend als de Netscaler ADC. Ook betreft het de Citrix Gateway die eerder bekend stond als de Netscaler Gateway. Door de kwetsbaarheid kan een niet geauthenticeerde indringer willekeurige commando's uitvoeren. Sinds 9 januari 2020 is bekend dat aanvallers actief gebruik proberen te maken van dit lek. Voor die tijd waren er nog geen kwaadwillige exploits gevonden. Op 11 januari 202 werd duidelijk dat het kinderlijk eenvoudig was om van de kwetsbaarheid gebruik te maken. In Nederland zou het om ruim 700 via het publieke internet bereikbare Citrix ADC servers gaan. Daar zitten **naast overheidsinstellingen, meerdere zorginstellingen, zorgverzekeraars ook zorgaanbieders** bij. Een patch is vanaf 20 januari beschikbaar, maar systeembeheerders kunnen nu al maatregelen nemen.

CVE-2019-19781

Kwetsbaarheden in hard- en software worden bijgehouden in een Amerikaanse database. Dat is de National Vulnerability Database(NVD) die de Common Vulnerabilities and Exposures(CVE) bijhoudt. De genoemde Citrix-kwetsbaarheid kreeg als nummer CVE-2019-19781. Deze informatie deelt men wereldwijd. Daarop

kan dan geacteerd worden. De praktijk wijst helaas uit dat het handelen hiernaar door organisaties vaak niet de hoogste prioriteit heeft. Systeembeheerders kunnen of zelf laks zijn, of door de leiding afgehouden worden van alert reageren. Zulks op basis van het korte termijn denken dat de werking van de systemen voor de klanten niet door dit zeer noodzakelijk onderhoud onderbroken mag worden. Helaas is zeer recent duidelijk geworden dat zoiets tot grote narigheid leidt.

Gevaar van niet reageren

Op 3 september 2019 schreef ik een artikel waarin ik refereerde aan een hot item: een kwetsbaarheid in kwetsbare Pulse Connect Secure SSL-VPNs in Nederlandse IP-adresruimte. Een aantal mensen uit de Nederlandse cybersecurity-scene die de gevaren ervan zagen, deden veel moeite om systeembeheerders van bedrijven te waarschuwen. Daar zaten overheidsinstellingen bij, maar ook instellingen en bedrijven van allerlei pluimage, ook uit de zorg. Heel recent bleek dat het grenswisselkantoor GWK Travelex getroffen was door ransomware. **Bij onderzoek kwamen zeven ungepatchte Pulse Connect servers aan het licht. En dat terwijl de softwarepatch beschikbaar was en men gewaarschuwd was.** Het toont genadeloos aan hoe kortzichtig het kan zijn om niet meteen in te grijpen. Nu zit GWK Travelex met een volledig versleuteld netwerk. Daarnaast is meer dan 5 GB aan persoonlijke data gestolen, waaronder geboortedata, social-security-nummers, betaalkaartgegevens en andere zaken. Voor het ontsleutelen van de data eisen de aanvallers 3 miljoen dollar.

Welke soorten instellingen nu?

Tot nu toe zijn ruim 700 via het publieke internet bereikbare kwetsbare Citrix ADC servers bekend. Net zoals bij de Pulse Connect kwetsbaarheid zitten er bij het Citrix-gebeuren **veel zorgaanbieders bij. Ziekenhuizen, GGZ-instellingen (waaronder een verslavingskliniek), een paar zorgverzekeraars, en**

meerdere doelgroep-zorgaanbieders (bijv. ouderen). Uiteraard zijn er ook weer een aantal hits bij Rijksoverheid-systemen. Hoewel de softwarepatch voor de Citrix-kwetsbaarheid nog niet voorhanden is kunnen systeembeheerders de configuratie van de Citrix ADC en andere hierboven genoemde apparaten wel zodanig wijzigen dat het gevaar substantieel minder is. Ook kan men voorbereidingen treffen om de binnenkort beschikbare patch te installeren. Op Nu.nl was op 13 januari 2020 hierover ook een item te zien.

Dutch Institute of Vulnerability Disclosure

Juist voor dit soort situaties is zeer recent, in de herfst van 2019 het Dutch Institute of Vulnerability Disclosure(DIVD) opgericht. Het is een netwerk van cybersecurity-researchers, vrijwilligers die voornamelijk online werken. Er is geen fysiek kantoor . Bij kwetsbaarheden in hard- of software is gebleken dat het Nationaal Cyber Security Centrum(NCSC) zich eigenlijk voornamelijk richt op de overheid en vitale infrastructuur. Juist ten aanzien van acties richting een brede groep gebruikers in bedrijfsleven, dienstensector en non-profit-organisaties is gerichte actie nodig om kwetsbaarheden dringend onder de aandacht te brengen. Binnen DIVD is men gestart met het Nederlands Security Meldpunt (in oprichting). Het is een groep vrijwilligers, onderdeel van het DIVD, die het zich tot taak heeft gesteld eigenaren van Nederlandse netwerkblokken en websites te informeren over (cyber)security-zaken die bij het meldpunt gemeld worden. Over de Citrix-kwestie verscheen op 13 januari 2019 ook een bericht. Het zijn loffelijke initiatieven.

Actie

Het is nu zaak dat systeembeheerders en cybersecurity-specialisten in de zorg in de eerste plaats nagaan of ze Citrix ADC apparaten in hun configuratie hebben staan en in de

tweede plaats actie ondernemen om het gevaar te beperken en op scherp te staan als de beveiligingspatch zeer binnenkort beschikbaar is.

W.J. Jongejan, 14 januari 2020

Afbeelding van Sarah Richter via Pixabay