TLP:WHITE

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC Maandmonitor

september 2021

Maandelijks analyseert het NCSC de belangrijkste ontwikkelingen op het gebied van digitale veiligheid. Dit document beschrijft deze ontwikkelingen voor de maand september 2021. Naast de feitelijke ontwikkelingen zijn in dit document ook links naar de bronnen [🖱] en commentaren van het NCSC opgenomen. Zie de "NCSC Maandmonitor Bijsluiter" voor meer uitleg over dit product en de verspreidingsvoorwaarden.

Conti-ransomware

In de Verenigde Staten nemen ransomware-aanvallen met Conti-ransomware toe. Dat concluderen de Amerikaanse CISA, FBI en NSA gezamenlijk in een waarschuwing. [🖱1] Volgens diverse mediaberichten heeft een ontevreden teamlid van Conti een draaiboek uitgelekt. [🖱2] [🖱3]
Naast de waarschuwing hebben de bovenstaande Amerikaanse instanties ook een beveiligingsadvies over Conti gepubliceerd. [🖱4] Dit advies geeft onder meer inzicht in de gebruikte tactieken, technieken en procedures (TTP's). Ter bescherming tegen Conti-ransomware beschrijft het advies een aantal (basis)maatregelen zoals het implementeren van multifactorauthenticatie, segmentering en isolatie van netwerken en het tijdig updaten van systemen.
In juli lanceerde CISA met partners de Stop Ransomware campagne. [🖱5] Het doel is het bewustzijn vergroten door organisaties te helpen met het aanbieden van factsheets, webinars en best practices op het gebied van security en risicomanagement. Eerder dit jaar is in Nederland een Taskforce Ransomware opgericht door de politie en partners om ransomware beter te kunnen bestrijden. [🖱6]

- *In de maand augustus waarschuwde het NCSC onder andere in de maandmonitor voor misbruik van ProxyLogon en Proxyshell. Bovenstaande illustreert dat criminelen dankbaar gebruik maken van kwetsbaarheden die door organisaties niet of te laat gepatcht worden. Zorg dat uw patchbeleid is ingericht.*
- *In de NCSC Handreiking Cybersecuritymaatregelen, kunt u aanvullende maatregelen vinden om de weerbaarheid van uw organisatie te vergroten. [🖱7]*
- *Het NCSC onderschrijft de adviezen die CISA heeft gepubliceerd.*

NBV waarschuwt voor komst kwantumcomputers

Op 23 september heeft het Nationaal Bureau voor Verbindingsbeveiliging (NBV) van de AIVD een brochure gepubliceerd over de dreiging die uitgaat van kwantumcomputers. [🖱8] Het NBV acht de kans klein maar reëel dat er in 2030 een kwantumcomputer bestaat die onze huidige cryptografie kan kraken. Gezien het probleem van 'store and decrypt' is het zeker voor vertrouwelijke informatie met een lange gevoeligheidstermijn van belang om nu al passende maatregelen te treffen. Naast de recente brochure van het NBV biedt ook de publicatie 'Factsheet Postkwantumcryptografie' van het NCSC aanvullend handelingsperspectief. [🖱9]

- *Hoewel het bij symmetrische cryptografie zoals de Advanced Encryption Standard (AES) of ChaCha20 relatief makkelijk is om over te stappen van 128-bit sleutels naar 256-bit sleutels om een systeem resistent te maken tegen kwantumcomputers is dit niet het geval met asymmetrische cryptografie zoals RSA en Diffie-Hellman. Daarvoor zijn nieuwe algoritmes nodig. Zoals rond de eeuwwisseling ook voor AES is gedaan heeft het Amerikaanse National Institute of Standards and Technology (NIST) in 2016 een competitie uitgeschreven om kwantumresistente asymmetrische algoritmes te standaardiseren. [🖱10] Eind 2021 of begin 2022 wordt van NIST een eerste selectie verwacht met algoritmes die gestandaardiseerd zullen worden. Deze dienen daarna te worden omgebouwd tot standaarden en implementaties. Wel zijn er nu al standaarden beschikbaar om traditionele gestandaardiseerde cryptografie te combineren met experimentele kwantumresistente algoritmes in een zogeheten hybride constructie. [🖱11] [🖱12] Gezien efficiënte (implementaties van) kwantumresistente algoritmes nog relatief nieuw zijn en nieuwe risico's met zich meebrengen is het verstandig om een dergelijke hybride constructie toe te passen.*

Speurtocht naar serieuze kwetsbaarheden

Binnen de internationale cybersecurity community heerst een grote bereidheid om kwetsbaarheden te vinden en bij te dragen aan de veiligheid van ICT-systemen. Hierbij wordt vaak samengewerkt in onderzoeken en heeft tot doel om de algehele beveiliging van systemen en producten te verbeteren. Bugbounty-programma's blijven een onverminderd populair middel om dit te bewerkstelligen. [13] Zo heeft gemeente Den Haag deze maand bijvoorbeeld voor de vierde keer 'Hâck The Hague' georganiseerd. [14]
Deze maand heeft een beveiligingsonderzoeker drie kwetsbaarheiden in iOS van Apple gevonden en publiek gemaakt. [15] Een andere beveiligingsonderzoeker onthulde op de dag dat Apple iOS 15 uitbracht de details van een kwetsbaarheid om het iPhone-vergrendelingsscherm te omzeilen. [16]

- *De door de onderzoekers vrijgegeven informatie stelt iedereen met de juiste vaardigheden in staat om misbruik te kunnen maken van de kwetsbaarheden in iOS.*
- *Het NCSC geeft in de factsheet 'Coordinated Vulnerability Disclosure' richtlijnen om als organisatie een CVD-beleid in te richten. Hierin wordt geprobeerd een balans te vinden tussen het belang om kwetsbaarheden zo snel mogelijk bekend te maken, zodat men maatregelen kan treffen, en het belang van ontwikkelaars en leveranciers om voldoende tijd te hebben de kwetsbaarheid te verhelpen. [17]*

De ONE, in één woord……

Op 28 en 29 september is de cybersecurityconferentie de ONE weer gehouden in Den Haag. Dit jaar werd het georganiseerd door het ministerie van Economische Zaken en Klimaat, de gemeente Den Haag en het NCSC. [18] De ONE werd dit jaar in een hybride vorm gegoten zodat zoveel mogelijk mensen het programma fysiek en/of virtueel konden bijwonen. [19] Diverse cybersecurity-experts spraken over uitdagingen en innovatieve oplossingen in het digitale domein. [20] Zo kwamen onder andere de onderwerpen ransomware, cyber threat intelligence (CTI), digitale soevereiniteit en supplychain-risico's aan bod. De laatste dag werd afgesloten met een slotwoord van demissionair minister Grapperhaus en een liveoptreden waarbij de boodschap duidelijk was, we moeten ons samen sterk (blijven) maken voor cybersecurity!

- *Heb je de ONE gemist en wil je toch graag de presentaties terugkijken? In het e-magazine is de link te vinden om de gewenste sessies terug te kijken. [21] De samengevatte sfeerimpressie van de twee dagen staat ook online. [22]*

Overig nieuws Nederland

Dagelijks bedrijven plat door ransomware [23] ■ NCSC publiceert factsheet 'PKIoverheid stopt met webcertificaten: Kies een andere leverancier' [24] ■ Onderwijsinspectie: Digitale weerbaarheid in het hoger onderwijs moet beter [25] ■ ESET highlights aggressive ransomware tactics and intensifying password-guessing attacks [26] ■ CoronaCheck-app soms onbereikbaar door DDoS-aanvallen en grote drukte [27] ■ Evaluatie internationaal cybersecuritybeleid van het ministerie van Buitenlandse Zaken [28] ■ Kwetsbaarheid in Apple Pay maakt betaling met vergrendelde iPhone mogelijk [29] ■ Verhoogde budgetten voor AIVD, MIVD en politie om cybercapaciteit te versterken en cybercrime aan te pakken [30] ■ Milieudienst: Cybersecurity niet op orde bij bedrijven met gevaarlijke stoffen [31] ■ FamousSparrow spioneert bij o.a. overheden en private partijen [32] ■ RTL Nederland betaalt hackers 8500 euro na ransomwareaanval [33] ■