Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

End of Week

vrijdag 24 mei 2024

Toegestane verspreiding: TLP:GREEN
(Traffic Light Protocol)

Deze handreiking bevat het label TLP:GREEN en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp). Ontvangers mogen de informatie delen met collega's van andere organisaties, informatiefora of personen werkzaam in netwerkbeveiliging, informatiebeveiliging of de VI-gemeenschap in de bredere zin. Het is niet de bedoeling dat u de informatie publiek maakt.

Uw reacties zijn welkom op info@ncsc.nl

Welkom bij de End of Week van vrijdag 24 mei 2024.

We gaan het eerst hebben over de Internetconsultatie Cyberbeveiligingswet en Wet weerbaarheid kritieke entiteiten die dinsdag van start ging. Gevolgd door de toekomstvisie op publiek-private samenwerking en tot slot gaan we het over nieuwe anti-ransomware plannen van het Verendig Koninkrijk hebben.

Internetconsultatie Cyberbeveiligingswet en Wet weerbaarheid kritieke entiteiten van start

Op 21 mei 2024 is de internetconsultatie gestart van de Cyberbeveiligingswet en de Wet weerbaarheid kritieke entiteiten. De consultatieperiode loopt tot 2 juli 2024. De wetsvoorstellen zijn de omzetting van twee Europese richtlijnen: de Network and Information Security Directive (NIS2) en de Critical Entities Resilience Directive (CER) naar nationale wetgeving. Deze hebben als doel om de fysieke, digitale en economische weerbaarheid te versterken tegen toenemende dreigingen.

Via www.internetconsultatie.nl kan iedereen suggesties doen voor verbetering van de wet- en regelgeving in voorbereiding. Het doel van de consultatie is een zo groot mogelijke groep van burgers, bedrijven en instellingen te betrekken bij de totstandkoming van de wetgeving. Op deze wetsvoorstellen kan tussen 21 mei 2024 en 2 juli 2024 worden gereageerd. Na afloop van deze periode worden alle reacties bekeken en wordt eventueel het wetsvoorstel aangepast. Het resultaat van de consultatie en de verwerking daarvan wordt in een verslag op hoofdlijnen vermeld op de website.[1]

Toekomstvisie op publiek-private samenwerking voor digitaal veilig Nederland

De digitale dreiging voor Nederland is groot en verandert voortdurend. Het is daarom van essentieel belang dat overheid, bedrijven en maatschappelijke organisaties hun digitale weerbaarheid op orde hebben. Dat vergt intensievere, bredere en eenduidigere publiek-private samenwerking. Om daartoe te komen heeft het kabinet een toekomstvisie opgesteld voor een publiek-privaat Cyberweerbaarheidsnetwerk.

De publiek-private samenwerking op het gebied van digitale veiligheid wordt tot op heden vormgegeven in het Landelijk Dekkend Stelsel van cybersecurity samenwerkingsverbanden. De toekomstvisie van het kabinet beschrijft hoe de verschillende bestaande elementen van het Landelijk Dekkend Stelsel kunnen worden uitgebreid en versterkt tot het Cyberweerbaarheidsnetwerk. [2]

[1] https://www.nctv.nl/actueel/nieuws/2024/05/21/internetconsultatie-cyberbeveiligingswet-en-wet-weerbaarheid-kritieke-entiteiten-van-start

[2] https://www.nctv.nl/actueel/nieuws/2024/05/23/toekomstvisie-cyberweerbaarheidsnetwerk

Nieuwe aanpak ransomware in het Verendig Koningkrijk

Volgens Recorded Future News komt ook het Verenigd Koninkrijk binnenkort met nieuwe wetsvoorstellen en een daarbij behorende consulatie. Centraal staat een meldplicht voor alle organisaties die getroffen zijn door ransomware-aanvallen. Het NCSC-UK waarschuwde eerder al dat ze zich zorgen maken over slachtoffers van ransomware-aanvallen die dit geheim houden.[3]

Daarnaast zullen organisaties een vergunning moeten aanvragen om losgeld te mogen betalen. Voor organisaties binnen de vitale infrastructuur word het verboden om losgeld te betalen. Het idee hierachter is dat de financiële prikkel om zulk soort organisaties aan te vallen wordt weggenomen en de aanvallen hierdoor afnemen.[4]

Beveiligingsadviezen

Zie voor een actueel overzicht: https://advisories.ncsc.nl/advisories

NCSC-2024-0230 [1.00] [M/H]	Kwetsbaarheden verholpen in QNAP QTS en QTS Hero
NCSC-2024-0229 [1.00] [M/H]	Kwetsbaarheid verholpen in QlikSense Enterprise
NCSC-2024-0231 [1.00] [M/H]	Kwetsbaarheden verholpen in Atlassian producten
NCSC-2024-0232 [1.00] [M/H]	Kwetsbaarheden verholpen in Veeam Backup Enterprise Manager
NCSC-2024-0233 [1.00] [M/H]	Kwetsbaarheden verholpen in Cisco producten
NCSC-2024-0234 [1.00] [M/H]	Kwetsbaarheid verholpen in Github Enterprise Server

[3] https://therecord.media/uk-increasingly-concerned-of-ransomware-victims-keeping-quiet-ncsc

[4] https://therecord.media/uk-proposal-mandatory-reporting-ransomware-attacks

Wat was er nog meer in het nieuws

CVE-2024-4978: Justice AV Solutions Viewer kwetsbaar

Rapid7 heeft vastgesteld dat gebruikers met JAVS Viewer v8.3.7 een hoog risico lopen en onmiddellijk actie moeten ondernemen. Deze versie bevat een backdoor waarmee aanvallers volledige controle kunnen krijgen over de getroffen systemen.[5]

MediSecure cyber security incident

De Australische regering werkt samen met MediSecure, een voormalige nationale aanbieder van receptenbezorgdiensten, om te ondersteunen bij een groot cyberincident dat het bedrijf treft.[6] Volgens de Australische minister voor Cyber Security en de National Cyber Security Coordinator gaat het om een grote ransomware-aanval en zijn er persoonsgegevens ontvreemd.[7]

Staatshackers wenden zich tot enorme ORB-proxynetwerken om detectie te omzeilen

Beveiligingsonderzoekers waarschuwen dat aan de Chinese Staat gelieerde hackers voor cyberspionageactiviteiten steeds vaker gebruik maken van een enorm proxyservernetwerk dat is opgebouwd uit virtuele private servers en gecompromitteerde online apparaten. Deze proxy-meshes worden operational relay box (ORBs) networks genoemd en worden beheerd door onafhankelijke cybercriminelen die vervolgens toegang bieden aan verschillende Advanced Persistent Threats (APT's)[8].

Google verhelpt opnieuw actief aangevallen kwetsbaarheid in Chrome

Voor de achtste keer dit jaar heeft Google een noodupdate uitgebracht voor zijn Chrome-browser die een actief misbruikte zero-day-kwetsbaarheid (CVE-2024-5274) verhelpt.[9]

[5] https://www.rapid7.com/blog/post/2024/05/23/cve-2024-4978-backdoored-justice-av-solutions-viewer-software-used-in-apparent-supply-chain-attack/

[6] https://www.homeaffairs.gov.au/cyber-security-subsite/Pages/nat-cyber-security-coordinator/medisecure-cyber-security-incident.aspx

[7] https://x.com/ClareONeilMP/status/1791297918470856861

[8] https://www.bleepingcomputer.com/news/security/state-hackers-turn-to-massive-orb-proxy-networks-to-evade-detection/

[9] https://chromereleases.googleblog.com/2024/05/stable-channel-update-for-desktop_23.html

Uitgave
Nationaal Cyber Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

mei ’24

TLP:GREEN