Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

End of Week

vrijdag 21 juni 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

Voor je ligt de End Of Week van 21 juni met interessante nieuwsberichten van afgelopen week, waaronder een korte samenvatting van de cyberoefening Cyber Europe, alsmede een selectie van gepubliceerde beveiligingsadviezen.

Cyber Europe cyberoefening 2024

Op 19 en 20 juni heeft het NCSC meegedaan met Cyber Europe, de tweejaarlijkse cyberoefening georganiseerd door ENISA. Het scenario richtte zich dit jaar op grootschalige problemen in de energiesector, waarbij stroomuitval, onbereikbaarheid van cruciale systemen en reputatieverlies een grote rol speelden.

Het NCSC oefende mee met een operationeel team van 15 collega's. Vanuit de energiesector deden zowel crisisteams als technisch specialisten van een aantal grote energiebedrijven en netwerkbeheerders. Ook de NCTV deed mee aan de oefening met een vertegenwoordiger voor het Europese CyCLONe netwerk, de bestuurlijke tegenhanger van het CSIRTs Network.

De oefendoelen van het NCSC bestonden uit het oefenen van een operationele opschaling, het oefenen van de samenwerking met de energiesector en oefenen van samenwerking met EU lidstaten binnen het CSIRTs Network en met CyCLONe. (CyCLONe is het Europese netwerk van verbindingsorganisaties voor cybercrises)

Tijdens de tweedaagse oefening heeft het operationeel team van het NCSC vier crisisoverleggen gevoerd en een overleg met de sector georganiseerd, om het situationeel beeld met elkaar af te stemmen en elkaars behoeften in kaart te brengen. Er zijn verder diverse berichten verstuurd en er hebben meerdere calls binnen het opgeschaalde Europese CSIRTs Network plaatsgevonden. Ook zijn er volop technische artefacten geanalyseerd die vanuit het scenario beschikbaar werden gesteld.[1]

Quishing

Het is niet voor iedereen nieuws want het misbruiken van QR-codes is immers al enige tijd een welbekend fenomeen. Toch willen we aan deze vorm van phishing nog even aandacht besteden. Voor securityprogramma's zijn sommige kwaadaardige links in de QR-code niet als zodanig te herkennen. Dit heeft voornamelijk te maken met het feit dat de kwaadaardige links zijn opgebouwd uit HTML in de vorm van ASCII-tekens. Het lijkt erop dat deze vorm van Quishing aan een opmars bezig is.[2]

[1] https://www.enisa.europa.eu/topics/training-and-exercises/cyber-exercises/cyber-europe-programme/cyber-europe-2024

[2] https://www.channelconnect.nl/security-en-privacy/nieuwe-bedreiging-via-e-mail-quishing/

Beveiligingsadviezen

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

NCSC-2024-0263 [v1.00] [M/H]	Kwetsbaarheden verholpen in Autodesk Autocad
NCSC-2024-0262 [v1.00] [M/H]	Kwetsbaarheden verholpen in VMware vCenter

Wat was er nog meer in het nieuws

VMware vCenter-servers kwetsbaarheid

Er zijn twee kritieke kwetsbaarheden die op afstand de VMware v-Center-servers kunnen overnemen. Er zijn updates uitgebracht om de beveiligingslekken te verhelpen.[3]

Asus-routers over te nemen

Een aantal Asus-routers is kwetsbaar voor 'code execution'. De leverancier geeft helaas geen verdere details over de kwetsbaarheid of een CVE-nummer. In het artikel geeft security.NL aan in welke routers de beveiligingslek aanwezig is.[4]

Europol haalt 13 websites neer

Middels de joint operation HOPPER II zijn 13 websites neergehaald die in verband stonden met terroristische operaties. Een groot aantal Europese landen hebben hieraan meegewerkt.[5]

[3] https://www.security.nl/posting/846504/VMware+vCenter-servers+via+kritieke+kwetsbaarheid+op+afstand+over+te+nemen

[4] https://www.security.nl/posting/846046/Asus-routers+via+kritieke+kwetsbaarheid+op+afstand+over+te+nemen

[5] https://gbhackers.com/europol-taken-down-13-websites/

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

juni ’24

TLP:GREEN