Wat is een NCSC beveiligingsadvies?
Een NCSC beveiligingsadvies is een advies met informatie over een recent gevonden kwetsbaarheid of dreiging in een specifiek softwareproduct. Een NCSC-beveiligingsadvies wordt in de community ook wel advisory genoemd. In de meeste gevallen is een advisory geschreven op basis van een publicatie door de leverancier van het product. Mogelijk wordt een advisory geschreven naar aanleiding van een publicatie door een onderzoeker.

Het doel is te beschrijven wat de kwetsbaarheid inhoudt en wat er mogelijk kan gebeuren wanneer deze wordt uitgebuit. Een advisory is – indien mogelijk – voorzien van praktische informatie over het verhelpen van de kwetsbaarheid.

Hoe komt de inschaling van een beveiligingsadvies tot stand?
Om een beveiligingsadvies te geven wordt de mogelijke Kans en Schade van de kwetsbaarheid bepaald. Hiervoor gebruikt het NCSC een inschalingsmatrix. Onderaan deze pagina staan de criteria waarmee een inschaling tot stand komt. Deze matrix is gebaseerd op de matrices van Common Vulnerability Scoring System (CVSS), US-CERT, SANS Internet Storm Center en Microsoft.

Welke uitgangspunten hanteert het NCSC bij het bepalen van de Kans en Schade?
Omdat elke infrastructuur verschillend is, moet elke kwetsbaarheid opnieuw worden ingeschaald door de ontvangende organisatie. Dit wordt ook wel een herwaardering van de advisory genoemd.

De beveiligingsadviezen gebaseerd op de inschalingsmatrix geven alleen een reëel beeld indien voldaan is aan de volgende best practice punten:

- *Firewall*

Gebruik een firewall om alleen die poorten te maken waar een door beleid gedefinieerde en gedocumenteerde noodzaak voor bestaat.

- *Filtering op segment*

Maak gebruik van verschillende netwerksegmenten (bijvoorbeeld een beheerssegment, een productiesegment en een serversegment) afgescheiden door firewalls.

Verwijzing:

https://www.ncsc.nl/actueel/factsheets/achtergrondinformatie-over-storm-worm.html

https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html

- *Beveiliging van infrastructuurcomponenten*

Beveilig infrastructuurcomponenten zoals routers, switches en servers (bijvoorbeeld ILO interfaces en software voor beheer op afstand), zodat niet iedere netwerkgebruiker deze kan benaderen.

- *Gebruik van server*

Een server wordt alleen gebruikt om voorgedefinieerde diensten aan te bieden. De server wordt niet als werkstation gebruikt.

- *Anti-virus software*

Voorzien elke host – indien mogelijk- van anti-virussoftware. Dit geldt voor werkstations en servers, zoals file- en mailservers.

Verwijzing:

https://www.ncsc.nl/actueel/factsheets/achtergrondinformatie-over-storm-worm.html

- *Content filtering*

Controleer netwerkverkeer van en naar het internet zoveel mogelijk op kwaadaardige inhoud.

Verwijzing:

https://www.ncsc.nl/actueel/factsheets/achtergrondinformatie-over-storm-worm.html

https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html

- *Versleuteling*

Gebruik de versleuteling van veilige protocollen (SFTP, SSH, HTTPS).

- *Geen standaard configuratie*

Maak zo min mogelijk gebruik van standaard configuratie van systemen. Verwijder bijvoorbeeld meegeleverde scripts in een IIS installatie en verander standaard wachtwoorden voor gebruik.

- *Gebruikers hebben geen Administrator rechten*

Gebruikers hebben geen Administrator of Root rechten op een werkstation.

Verwijzing:

https://www.ncsc.nl/actueel/factsheets/achtergrondinformatie-over-storm-worm.html

- *Beheeraccounts*

Gebruik aparte beheeraccounts voor beheertaken. Gebruik deze beheeraccounts niet om e-mails te versturen en ontvangen of om het internet te bezoeken.

- *Patchen*

Volg de beveiligingsadviezen op en installeer beschikbare en relevante patches of work-arounds om op die manier het gevaar op uitbuiting te minimaliseren.

- *Gebruikers bewustzijn*

Maak eindgebruikers bewust van de meest voorkomende beveiligingsrisico’s. Zorg er in ieder geval voor dat er niet op willekeurige links of mail attachments van onbekende wordt geklikt.

Verwijzing:

https://www.ncsc.nl/actueel/factsheets/achtergrondinformatie-over-storm-worm.html

- *Mobiele apparatuur is voorzien van beveiligingsmaatregelen*

Bereid mobiele apparaten, zoals laptops, voor en breng ze op hetzelfde beveiligingsniveau als de werkstations binnen uw organisatie.

Verwijzing:

https://www.ncsc.nl/actueel/factsheets/factsheet-veilig-gebruik-van-smartphones-en-tablets.html

- *Belangrijke systemen zijn fysiek beveiligd*

Zorg voor fysieke beveiliging van belangrijke systemen, zoals servers en infrastructuurcomponenten.

- *Geen vreemde hardware op het netwerk*

Zorg ervoor dat er alleen hardware aanwezig is op het netwerk die is aangekocht en/of beheerd door uw organisatie. Laat geen laptops van externe medewerkers toe op het productie LAN. Controleer bijvoorbeeld regelmatig of er illegale hardware (zoals ongeautoriseerde Wireless Access Points) aanwezig is.

Waarom zijn bepaalde NCSC beveiligingsadviezen niet beschikbaar/leesbaar?
Het kan zijn dat het NCSC een beveiligingsadvies schrijft op basis van informatie die van haar bron alleen gedeeld mag worden met de primaire doelgroep van het NCSC, zoals de Rijksoverheid en vitale sectoren. Beveiligingsadviezen worden daarom niet altijd gepubliceerd.