Nationaal Cyber Security Centrum
*Ministerie van Justitie en Veiligheid*

# End of Week

## vrijdag 29 december 2023

**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 u ligt de End of Week van 29 december en daarmee ook de laatste van dit jaar.*

*Er kwam deze week veel informatie vanuit het ministerie van Binnenlandse Zaken en Koninkrijksrelaties over digitalisering en daar attenderen we u graag op. Het was rustig deze week wat betreft beveiligingsadviezen. Er verschenen slechts twee deze week. Verder komen HTTPS en SQL injection nog aan bod.*

*We wensen u een heel fijn weekend en een veilig en gezellig nieuwjaar!*

## Digitalisering wacht op niemand

De ministerraad heeft op voorstel van staatssecretaris Van Huffelen (Koninkrijksrelaties en Digitalisering) ingestemd met toezending aan de Tweede Kamer van de verzamelbrief digitalisering. In de brief staat onder andere de voortgang op de doelstellingen en actiepunten uit de in het afgelopen jaar gepresenteerde Werkagenda Waardengedreven Digitaliseren en de plannen voor 2024. Een aantal onderwerpen uit de brief:

**Principebesluit 'gov.nl'**

Vertrouwen in de digitale wereld is een belangrijke voorwaarde om volledig mee te kunnen doen. Op grond van veiligheidsoverwegingen en internationale voorbeelden heeft het kabinet een principebesluit genomen om te kiezen voor de overheidsextensie '.gov.nl.'.

Naast de uniforme domeinnaamextensie werkt het kabinet ook aan het Register Internetdomeinen Overheid (RIO) als bron waar burgers terechtkunnen voor een snelle check op de echtheid van overheidswebsites.

**Veilig gebruik van AI**

Als het gaat om gebruik van generatieve AI door Rijksorganisaties is het recente advies dat alleen te doen als er aantoonbaar wordt voldaan aan geldende wet- en regelgeving. Het kabinet wil daarom het gebruik van generatieve AI binnen de overheid en in de verschillende sectoren op een veilige en verantwoorde manier bevorderen. Om die reden verschijnt in januari 2024 de kabinetsbrede visie op generatieve AI.

**Versterken CIO Rijk**

Volwaardige digitalisering van de overheid is vereist voor succes in de eerste 3 lijnen van de werkagenda en ook om als overheid zelf, intern én naar buiten toe, goed te kunnen functioneren. Daarvoor moet de overheid open en gedreven door publieke waarden werken. Een andere manier om de verantwoorde inzet van digitalisering te verbeteren is het versterken van het stelsel voor Chief Information Officers (CIO). Deze zijn verantwoordelijk voor de digitalisering binnen de Rijksoverheid. Het kabinet wil de rol van de CIO in 2024 verder versterken en daarmee hen in staat stellen om ervoor te zorgen dat bijvoorbeeld de informatiehuishouding op orde is, de kwaliteit van IT-systemen wordt verbeterd, problematische legacy wordt aangepakt en de digitale dienstverlening steeds beter wordt. Daarom zal het CIO-stelsel geëvalueerd en herzien worden. Daarbij wordt in het bijzonder gekeken naar de coördinerende rol van CIO Rijk.

**Digitale vaardigheden en kennis**

Iedereen moet kunnen meedoen in de digitale samenleving. Daarvoor is het nodig

dat iedereen over volgende digitale vaardigheden en kennis beschikt. Het beleid is daarom gericht op het bereiken van digitale inclusie. Het Centraal Bureau voor de Statistiek (CBS) en Eurostat onderzoeken in het onderzoek 'ICT-gebruik van huishoudens en personen' eens per twee jaar het percentage Nederlanders dat digitale vaardigheden bezit in relatie tot andere Europese landen. Volgens de meting van 2023 beschikt 83% van de Nederlanders van 16 tot 75 jaar over ten minste digitale basisvaardigheden. [1, 2]

## Volledig versleuteld web dichtbij, maar groei HTTPS-sites stagneert

Een groot deel van het web is nu versleuteld via HTTPS, maar de groei van het aantal HTTPS-sites lijkt te stagneren. Volgens Google gebruikt 95 procent van het web HTTPS, terwijl Firefox dit op 80 procent schat. De Amerikaanse burgerrechtenbeweging EFF wijst op verschillende redenen waarom nog steeds een deel van de websites via HTTP wordt geladen, zoals verouderde sites, bewuste keuzes van sommige websites, beperkte ondersteuning en toegankelijkheidsobstakels voor het verkrijgen van TLS-certificaten. De EFF benadrukt ook het belang van versleuteling in mobiele apps als het volgende strijdgebied, maar gelooft uiteindelijk dat een volledig versleuteld web mogelijk is.[3]

## SQL injection bestaat 25 jaar

Security.nl kwam eerste kerstdag met een mooi artikel over SQL injection die ook op die dag een soort 25ste verjaardag vierde. Er wordt ingegaan op de werking, historie, en de hedendaagse manifestatie van deze kwetsbaarheid. "MITRE, de organisatie achter het Common Vulnerabilities and Exposures (CVE) systeem om kwetsbaarheden mee te identificeren, publiceert elk jaar een Top 25 van de gevaarlijkste kwetsbaarheden. Net als vorig jaar staat SQL injection dit jaar wederom in de top drie."[4]

[1] https://www.rijksoverheid.nl/actueel/nieuws/2023/12/22/digitalisering-wacht-op-niemand

[2] https://www.rijksoverheid.nl/documenten/kamerstukken/2023/12/22/verzamelbrief-digitalisering-december-2023

[3] https://www.security.nl/posting/823391/Volledig+versleuteld+web+dichtbij%2C+maar+groei+HTTPS-sites+stagneert

[4] https://www.security.nl/posting/823251/SQL+injection+bestaat+25+jaar%253A+nog+overal+aanwezig+en+zeer+effectief

## Beveiligingsadviezen

*Zie voor een actueel overzicht: www.ncsc.nl/actueel/beveiligingsadviezen*

| | |
|---|---|
| NCSC-2023-0657 [1.00][M/M] | Kwetsbaarheid verholpen in Google Chrome |
| NCSC-2023-0654 [1.01][M/H] | Kwetsbaarheden verholpen in OpenSSH |

## Wat was er nog meer in het nieuws

### Kabinet onderzoekt effectiviteit landelijke wervingscampagne ICT'ers

"Het kabinet laat onderzoeken hoe effectief het is om een landelijke campagne te voeren voor het werven van ICT'ers. De kosten van een wervingscampagne kunnen uiteen lopen van enkele tonnen tot tientallen miljoenen euro's per jaar. Het kabinet wil dat er in 2030 één miljoen ict'ers in Nederland zijn, ook wel 'digitaal geschoolden' genoemd."[5]

### Duitse ziekenhuizen sluiten spoedeisende hulp na ransomware-aanval

"Drie Duitse ziekenhuizen hebben vanwege een aanval met de LockBit-ransomware besloten de spoedeisende hulp tijdelijk te sluiten. Systemen van het Franziskus Hospital Bielefeld, Sankt Vinzenz Hospital Rheda-Wiedenbrück en Mathilden Hospital Herford raakten dit weekend geïnfecteerd waarbij allerlei data werd versleuteld."[6]

### Australische tak Yakult slachtoffer van ransomware-aanval

"De Australische tak van de Japanse probioticaproducent Yakult is slachtoffer van een ransomware-aanval geworden. Op 21 december meldde een ransomwaregroep genaamd 'DragonForce' dat het een aanval op Yakult had uitgevoerd en dat daarbij bijna honderd gigabyte aan data is buitgemaakt."[7]

### Kwetsbaarheid in interpretatie SMTP-protocol maakt gespoofte e-mails mogelijk

"Een kwetsbaarheid in de interpretatie van het SMTP-protocol maakt het mogelijk om vanaf allerlei domeinen gespoofte e-mails te versturen en zo phishingaanvallen uit te voeren. Daarvoor waarschuwt securitybedrijf SEC Consult, dat de gebruikte methode 'SMTP smuggling' noemt."[8]

---

[5] https://www.security.nl/posting/823396/Kabinet+onderzoekt+effectiviteit+landelijke+wervingscampagne+ICT%27ers

[6] https://www.security.nl/posting/823472/Duitse+ziekenhuizen+sluiten+spoedeisende+hulp+na+ransoware-aanval

[7] https://www.security.nl/posting/823375/Australische+tak+Yakult+slachtoffer+van+ransomware-aanval

[8] https://www.security.nl/posting/822364/Kwetsbaarheid+in+interpretatie+SMTP-protocol+maakt+gespoofte+e-mails+mogelijk

**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

december ’23

TLP:GREEN