Nederlandse Emissieautoriteit
Dutch Emissions Authority

Februari 2022

Veiligheidsmaatregelen voor gebruikers NEa-register

Dit informatieblad is bedoeld voor gebruikers van de registers die de Nederlandse Emissieautoriteit (NEa) beheert. De NEa spant zich in om de registers te beveiligen tegen ongewenst gebruik. Ook u als gebruiker speelt een belangrijke rol in de beveiliging van de registers. In dit informatieblad leest u alles over maatregelen die u kunt nemen om de registers veilig te gebruiken.

De NEa beheert drie registers:

- het Europese Register voor handel in emissierechten (EU ETS-register) in samenwerking met de Europese Commissie;
- het Register Energie voor Vervoer (REV) voor handel in Hernieuwbare Brandstofeenheden (HBE's).
- het CO2-heffingsregister (CHeR) voor handel in dispensatierechten en het doen van aangifte voor de CO2-heffing industrie.

Meer informatie over de systemen van emissiehandel, energie voor vervoer en de registers vindt u op www.emissieautoriteit.nl.

Achtergrond

Kwaadwillenden hebben in het verleden verhandelbare eenheden in het vizier gekregen als doelwit van fraude en diefstal. De NEa spant zich samen met nationale en internationale partners in om te voorkomen dat criminelen succes boeken. In dit informatieblad geven wij u handvatten om te voorkomen dat kwaadwillenden via uw computer toegang krijgen tot uw rekening in het EU ETS-register, het REV en CHeR.

Maatregelen voor iedereen

Het is belangrijk dat u de onderstaande maatregelen in acht neemt als u gebruik gaat maken van een register. Deze maatregelen kunt u zonder grote moeite of investering nemen.

Algemene maatregelen

- Als u e-mails ontvangt uit naam van de NEa, controleer dan of de NEa daadwerkelijk de afzender is. Hoe u dit doet, leest u in het blokje *'Controle communicatie'* verderop in dit informatieblad.
- Als u in de communicatie met de NEa (via e-mail, telefoon, documenten of andere middelen) of tijdens het gebruik van een register iets verdachts opmerkt, neem dan direct contact op met de Helpdesk NEa. Contactgegevens van de helpdesk vindt u achterin dit infoblad.
- Gebruik geen programma's die online bestanden delen (bijvoorbeeld BitTorrent). Kwaadwillenden kunnen via deze programma's toegang krijgen tot uw computersysteem.
- Gebruik alleen vertrouwde USB-sticks op de computer waarmee u inlogt op een register. Via niet-vertrouwde sticks kan uw computersysteem besmet worden met virussen.

- Controleer regelmatig de transactiegeschiedenis van uw rekening op verdachte transacties.

Maatregelen voor uw mobiele telefoon

- Wees voorzichtig met het delen van uw mobiele nummer met anderen. Dit verzwakt de beveiliging van de registers.
- Log nóóit vanaf uw mobiele telefoon in op een register. Het risico is dat u hiermee al uw gegevens prijsgeeft aan kwaadwillenden. Die gegevens zijn zowel uw gebruikersnaam, wachtwoord als de QR code met de mobiele EU login app.
- Stel een wachtwoord of pincode in om uw mobiele telefoon te vergrendelen.
- Raakt u uw telefoon kwijt? Laat dan direct uw simkaart blokkeren door de provider.
- Indien u gebruik maakt van een smartphone, zorg dan dat het besturingssystem ge-update blijft om de veiligheid te verhogen.
- Maak alleen contact met beveiligde wifi-netwerken; maak nooit contact met openbare wifi-netwerken.

  Meer over veilig gebruik van een smartphone vindt u op: Hoe beveilig ik mijn smartphone of tablet? (veiliginternetten.nl).

Maatregelen voorafgaand aan het inloggen

- Informeer uzelf over de beveiligingsrisico's van computer-, internet- en e-mailgebruik en maak uzelf de tips voor veilig computergebruik eigen. Doe dit bijvoorbeeld door Antwoord op vragen en hulp bij problemen. Voor iedereen. (veiliginternetten.nl) te bestuderen. Beveilig uw computer optimaal en gebruik deze zo veilig mogelijk.
- Zorg dat op het computersysteem waarmee u wilt inloggen op een register:
  - altijd de meest recente updates van het besturingssysteem geïnstalleerd zijn;
  - een virusscanner geïnstalleerd is die steeds wordt bijgewerkt met de laatste virusdefinities en die het systeem minstens elke week volledig scant op virussen;
  - geen illegale software geïnstalleerd is.
- Als u gebruikmaakt van een wifi-netwerk, zorg dan dat u dit goed beveiligt. Openbare wifi-netwerken zijn niet veilig: Hoe maak ik veilig gebruik van openbare wifi-netwerken? (veiliginternetten.nl)
- Beveilig de toegang tot uw computer met een wachtwoord.
- Kies voor de toegang tot uw computer en de registers sterke wachtwoorden, zie het blokje *Wat is een sterk wachtwoord?.* Als u de wachtwoorden niet kunt onthouden, bewaar ze dan in een gerenommeerde wachtwoordmanager. Bewaar ze nooit op dezelfde plek als uw gebruikersnamen en sla ze nooit op in een onbeveiligd bestand op uw computer.
- Deel uw gebruikersnaam, wachtwoord en de QR gegenereerde beveiligingscodes nooit met anderen, ook niet met collega's. De NEa zal nooit om uw wachtwoord of beveiligingscode vragen.

Maatregelen tijdens het inloggen en gebruik

- Maak bij voorkeur gebruik van de browsers Firefox of Chrome. Het REV werkt niet optimaal in Internet Explorer.
- Log altijd in via de link naar een register die door de NEa gecommuniceerd wordt. Klik nooit op een andere link naar een register vanwege het risico dat u een nepsite voorgeschoteld krijgt waarop u uw inloggegevens achterlaat.
- Laat anderen niet meekijken als u uw gebruikersnaam en wachtwoord intoetst.

- Log altijd eerst uit voordat u wegloopt van uw computer. Vergrendel uw systeem (op een Windows-systeem via de toetscombinatie Windows-toets + L), zodat anderen hier tijdens uw afwezigheid niet bij kunnen.
- Sta uw browser nooit toe uw gebruikersnaam en wachtwoord op te slaan.
- Indien u verdachte activiteit op uw rekening in het REV constateert of vermoedt dat een onbevoegd persoon toegang heeft gekregen tot uw rekening in het REV, kunt u zelf uw rekening direct blokkeren. Ga na het inloggen naar Mijn REV → tabblad Mijn rekening en klik op de knop Rekening blokkeren (onder het kopje Toegang).

eHerkenning en CHeR

eHerkenning is een middel om veilig in te loggen bij overheidsdiensten en is nodig om in te loggen in CHeR.
Elke installatie waarop de CO2-heffing industrie van toepassing is, krijgt de beschikking over één rekening in CHeR. De rekeninghouder van de rekening in CHeR is de exploitant van de installatie, hier kan niet van worden afgeweken. Daarnaast kent CHeR geen contactpersonen, maar rekeningbevoegden. Vooralsnog is CHeR de enige NEa dienst waar u dient in te loggen met eHerkenning.

Aandachtspunten voor inloggen in CHeR met eHerkenning

- De tekenbevoegde of de aangestelde machtigingenbeheerder van de exploitant, is verantwoordelijk voor het beheer van machtigingen voor rekeningbevoegdheid in eHerkenning.
- De rekeningbevoegden zijn verantwoordelijk voor **veilig gebruik** van eHerkenning als inlogmiddel.
- De rekeningbevoegden zijn ook verantwoordelijk voor **veilig gebruik** van CHeR, waarbij de algemene aandachtspunten, zoals in de rest van dit document genoemd staan, in acht dienen te worden genomen.

Controle communicatie

De NEa, en in het geval van het EU ETS-register de Europese Commissie, hebben een aantal maatregelen genomen waardoor u kunt nagaan of de informatie die u leest en de berichten die u ontvangt betrouwbaar zijn.

Websites

Om er zeker van de zijn dat u veilig werkt in het juiste register en dat u de goede informatie krijgt, raden wij u aan twee stappen uit te voeren bij het bezoeken van onze websites.

1. Controleer het internetadres (de url) van de websites. Dit moet beginnen met:
   - NEa-website: https://www.emissieautoriteit.nl
   - EU Login-website voor inloggen register: https://webgate.ec.europa.eu/cas/
   - EU ETS-registerwebsite: https://ets-registry.webgate.ec.europa.eu/euregistry/NL/
   - Website REV: https://www.rev.emissieautoriteit.nl

2. Controleer de geldigheid van het certificaat van de bovengenoemde websites. Een geldig certificaat betekent dat u een veilige verbinding heeft met de website. Om dit te controleren, kijkt u of er een gesloten slotje zichtbaar is, links van de url. Hoe dit er precies uitziet verschilt per browser en is op de volgende websites aangegeven:
   - Firefox: https://support.mozilla.org/nl/kb/hoe-weet-ik-of-mijn-verbinding-is-beveiligd

- Chrome https://support.google.com/chrome/answer/95617?hl=nl
- Internet Explorer: http://windows.microsoft.com/nl-nl/windows/know-online-transaction-secure#1TC=windows-7
- Safari: https://support.apple.com/nl-nl/HT201756
- Opera: http://help.opera.com/opera/Windows/1781/en/private.html#certificates

Ziet u een gebroken slotje, een uitroepteken, een rood of zwart kruis of een ander waarschuwingssignaal i.p.v. een gesloten slotje? Ga dan niet verder met inloggen en neem contact op met de Helpdesk NEa.

E-mail
De NEa verstuurt berichten over de registers en de beveiliging daarvan altijd digitaal ondertekend:

- Klik op het certificaattekentje in de e-mail.
- Klik op 'Details'
- Klik op 'Gegevens bekijken'
- Klik op 'Certificaat weergeven'
- In het 'Certificeringspad' kunt u zien dat het certificaat afkomstig is van QuoVadis Issuing CA G3

Let op: soms wordt het certificaat als bijlage verzonden. Dit is vaak het geval als u berichten via webmail leest. U kunt deze controlestappen dan niet uitvoeren.

Verdergaande maatregelen
Als uw computer onderdeel is van een groot bedrijfsnetwerk, is de beveiliging ervan in handen van de ICT-beheerders van het netwerk. U kunt – behalve het treffen van de maatregelen die hierboven beschreven zijn – zelf weinig doen om uw computer beter te beveiligen. Wel kunt u dit informatieblad door de ICT-beheerders laten lezen en uzelf door hen laten verzekeren dat de netwerkomgeving veilig is. De onderstaande maatregelen kunt u overwegen als u werkt op een afzonderlijke computer of een netwerk gebruikt dat u zelf beheert.

- Overweeg voor de toegang tot een register een speciale computer waarmee u geen andere handelingen verricht dan het register benaderen en die niet (bijvoorbeeld via een netwerk) op andere computers is aangesloten. De kans op besmetting van uw computer met kwaadaardige software is hiermee een stuk kleiner.
- Overweeg om naast uw reguliere virusscanner een programma als IBM Security Trusteer Report (gratis) te installeren. Dergelijke programma's zijn speciaal gebouwd om virussen en andere malware op te sporen die gericht zijn op het achterhalen van inloggegevens of het overnemen van uw computer. Zij doen deze opsporing een stuk beter dan reguliere virusscanners.

Wat is een sterk wachtwoord?
U heeft een wachtwoord nodig om in te loggen op de registers. Wij raden u aan hier geen wachtwoord voor te gebruiken dat door derden makkelijk te achterhalen is. Een sterk wachtwoord in het register moet voldoen aan de volgende voorwaarden:

- minimaal 8 karakters lang;
- geen bestaand woord of een woord dat makkelijk te raden is, zoals de naam van uw kat of partner;
- bestaand uit:
    - hoofdletters
    - kleine letters
    - getallen
    - symbolen

Gebruik nooit hetzelfde wachtwoord voor verschillende toepassingen. Op https://veiliginternetten.nl/themes/situatie/mijn-wachtwoord-sterk-genoeg/ vindt u stappen voor het maken van een sterk wachtwoord.

Helpdesk NEa
Heeft u iets verdachts opgemerkt? Neem dan zo snel mogelijk contact op met de Helpdesk NEa per telefoon (070-339 52 50) of per e-mail *(info@emissieautoriteit.nl).*

Disclaimer
Aan de bovenstaande tekst kunt u geen rechten ontlenen. Ook is de NEa niet aansprakelijk wanneer er malafide activiteiten op uw rekening plaatsvinden.