

Vraag nu je cyberscan aan en zet die eerste stap!



Op <https://www.cvdnederland.nl/check>

Basisscan Cyberweerbaarheid - Digital Trust Center

voortgang: 0 %

› [Welkom](#)

- › 1. Inventariseer kwetsbaarheden
- › 2. Kies veilige instellingen
- › 3. Voer updates uit
- › 4. Beperk toegang
- › 5. Voorkom virussen en andere malware
- › Achtergrond & selectievragen

Is jouw basis op orde? Test het hier!

START

Publicatiedatum: 15-10-2024

Ben je een kleine mkb'er of zzp'er? Of wil je voor het eerst met de cybersecurity van je bedrijf aan de slag? Doe dan onze nieuwste cyberscan: **Cyberveilig Check voor mkb en zzp**. Deze zal beter aansluiten bij je verwachtingen.

[Naar de CyberVeilig Check voor mkb en zzp](#)

Is je basis op orde? Test het hier!

Ben je benieuwd of jouw onderneming de basis op orde heeft op het gebied van digitale veiligheid? Doe dan hier de Basisscan Cyberweerbaarheid!

Aan de hand van 25 stellingen kom je erachter hoe jouw onderneming scoort op de 5 Basisprincipes van veilig digitaal ondernemen, opgesteld door het Digital Trust Center (onderdeel van het ministerie van Economische Zaken).

**Modern Internet Standards provide for more reliability and further growth of the Internet.
Are you using them?**

Test your website



Modern address? Signed domain? Secure connection? Route authorisation?

[about the test](#) >

Your website domain name:

Start test

Test your email



Modern address? Anti-phishing? Secure transport? Route authorisation?

[about the test](#) >

Your email address:

Start test

Test your connection



Modern addresses reachable?
Domain signatures validated?

[about the test](#) >

Start test

News

Internet.nl available as 'ready-to-go'
Docker package >

Improved tests for CSP and security.txt >

Hall of Fame



5475 domains with 2 x 100%
Latest entry: 14-11-2024

✓ [p2hr.nl](#)

Tests in numbers

687762 unique web domains

✓ 100%: 43702

✗ 0-99%: 644060

Uitwijk- en herstelplan

Er zijn verschillende soorten incidenten die invloed kunnen hebben op je bedrijfsvoering. Incidenten kunnen variëren van een defecte printer tot een brand in je kantoorpand met mogelijk ernstige gevolgen. Incidenten zijn onverwacht en vinden helaas vaak op het verkeerde moment plaats.

We spreken van een **cyberincident** wanneer het incident de beschikbaarheid, integriteit of vertrouwelijkheid van informatiesystemen raakt. Hoe kun je je wapenen tegen cyberincidenten? Met een uitwijk- en herstelplan. Zo'n plan maakt dat je beter voorbereid bent en de schadelijke impact op je bedrijfsvoering kunt beperken.



Maritieme dienstverlener valt terug op een oud IT-systeem na hack

Na een cyberaanval vielen alle systemen van Roval Dirkzwager uit. Ook de geavanceerde



10 vragen voor je ICT-leverancier

- 1. Zijn de laatste beveiligingsupdates geïnstalleerd op alle programma's?**
Door te werken met de laatste versie loop je de minste kans op virussen en hacks. Deze maken namelijk gebruik van kwetsbaarheden in oudere versies van programma's. Het is van belang om alle updates direct uit te voeren.
- 2. Worden er regelmatig back-ups gemaakt en wordt er gecontroleerd of deze geslaagd zijn?**
Vraag zelf eens een restore aan van een bestand van een dag eerder ter controle.
- 3. Wordt er gebruikgemaakt van een virusscanner en firewall?**
Virusscanners en firewalls kunnen een deel van de hacks voorkomen. Installeer altijd de updates om te voorkomen dat nieuwe virussen een kans krijgen.
- 4. Zijn er logfiles beschikbaar (van o.a. de firewall)?**
Hieraan kun je zien wie wanneer heeft ingelogd. Ook kun je zien of jouw netwerk aangevallen wordt door hackers en op welke wijze dit heeft kunnen plaatsvinden.
- 5. Worden de medewerkers getraind in cybersecurity?**
Organisatorische maatregelen zijn minstens zo belangrijk als technische maatregelen om cybercrime te voorkomen. Het team is zo sterk als de zwakste schakel. Er hoeft maar één medewerker op een verkeerde link te klikken en de kans bestaat dat het hele bedrijf stil komt te liggen.
- 6. Worden mijn data versleuteld opgeslagen en kunnen persoonsgegevens indien gewenst verwijderd worden?**
Versleutelde data zijn geheel onleesbaar zonder de juiste sleutel, dus als iemand jouw bestanden steelt kunnen ze er niets mee doen. Het veilig opslaan en eventueel verwijderen van persoonsgegevens is ook van belang in het kader van de Algemene Verordening Gegevensbescherming (AVG).
- 7. Hoe vaak worden security testen gedaan en wat gebeurt er met de resultaten?**
- 8. Zijn er in het verleden security incidenten geweest?**
- 9. Waar worden mijn data opgeslagen en hoe is dit beveiligd?**
Er zijn landen buiten de EU die geen waarborg bieden voor een passend beschermingsniveau. Data kan zo in verkeerde handen vallen.
- 10. Wat wordt er gedaan zodra mijn bedrijf toch gehackt wordt?**
Maak vooraf afspraken over de inzet van jouw ICT-leverancier en ga er niet (zomaar) vanuit dat zij de hack oplossen.



Ministerie van Economische Zaken
en Klimaat

Afspraken maken met een IT-leverancier

Checklist Service Level Agreement

De veranderingen in het bedrijfsleven versnellen en we doen steeds vaker een beroep op technologie. Tegelijkertijd wordt technologie steeds complexer, waardoor je als ondernemer meer tijd kwijt bent aan het onderhouden van je technische omgeving, zoals

Uitbesteding kan flexibiliteit bieden, bijvoorbeeld als je tijdelijk extra laptops nodig hebt. Daarnaast kan het uitbesteden van IT kosten besparen doordat er geen directe kapitaalinvesteringen nodig zijn, zoals het in één keer aanschaffen van alle laptops en