economie
FOD Economie, K.M.O., Middenstand en Energie

Bent u een onderneming 1.0 of 2.0?

Doe de test en ontdek uw resultaten!

Om u te helpen bij het bepalen van de mate van maturiteit van uw onderneming voor cyberbeveiliging, vindt u hier een vragenlijst om uzelf te beoordelen, opgedeeld in twee delen:

Deel A. Organisatorische vragen (10 vragen)

Deel B. Technische vragen (10 vragen)

Kies voor elke vraag het antwoord dat u het meest geschikt vindt om de realiteit van uw onderneming weer te geven. Elk antwoord krijgt punten:

Onzeker (u weet het niet):	Geen punt
Nee:	1 punt
Ja, maar de uitvoering kan beter:	2 punten
Ja en de uitvoering is doeltreffend:	3 punten

De totale punten worden aan het eind van deze vragenlijst beoordeeld.

Om u te helpen cybersecurity beter te integreren in uw organisatie, verwijst elk van de vragen naar de relevante principes en acties die u kunt terugvinden in de handleiding *"Cyberveiligheid: Is uw bedrijf er klaar voor?"*

Begrijpt u bepaalde woorden of afkortingen niet? Aarzel dan niet om ook een kijkje in onze woordenlijst te nemen!

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

Deel A: Organisatorische vragen

1. Beschikt uw onderneming over een specifiek team of contactpunt dat instaat voor het beheer van de informatieveiligheid?

- (0) Onzeker
- (1) Nee
- (2) Ja, maar binnen het bedrijf weten weinigen met wie ze contact moeten opnemen of hoe ze deze persoon kunnen contacteren.
- (3) Ja en binnen het bedrijf weet iedereen tot wie hij zich moet wenden.

Om verder te gaan:

Onderneming 1.0

Principe 4. Laat zien dat u uw verantwoordelijkheid neemt

Onderneming 2.0

Actie 1. Betrek het topmanagement erbij

2. Uw onderneming verwerkt waarschijnlijk persoonlijke gegevens, maar heeft het een functionaris voor gegevensbescherming (DPO)?

- (0) Onzeker
- (1) Nee
- (2) Ja, maar u weet niet wie het is
- (3) Ja en u weet hoe u deze persoon moet contacteren

Om verder te gaan:

Onderneming 1.0

Principe 1. Leg de focus op informatie, niet op de technologie

Onderneming 2.0

Principe 4. Neem maatregelen met betrekking tot de bescherming van de persoonlijke levenssfeer

Actie 2. Publiceer een eigen veiligheidsbeleid en gedragscode

3. Heeft uw onderneming in de afgelopen drie maanden een risicoanalyse of een impactanalyse op het gebied van gegevensbescherming uitgevoerd?

- (0) Onzeker
- (1) Nee
- (2) Ja, maar u kent de resultaten niet
- (3) Ja en u bent op de hoogte van de corrigerende maatregelen die sindsdien zijn uitgevoerd

Om verder te gaan:

Onderneming 1.0

Principe 1. Leg de focus op informatie, niet op de technologie

Onderneming 2.0

Stap 1. Analyse van de risico's of "Ken uzelf"!

4. Heeft uw bedrijf een informatieveiligheidsbeleid voor het personeel (internet, sociale media, mobiele apparaten,...)?

- (0) Onzeker
- (1) Nee
- (2) Ja, maar dit beleid is niet bij alle personeelsleden bekend.
- (3) Ja en dit beleid maakt deel uit van de opleiding/sensibilisatie inzake cybersecurity voor werknemers.

Om verder te gaan:

Onderneming 1.0

Principe 5. Implementeer uw visie

Onderneming 2.0

Principe 2. Maak uw personeel bewust van informatieveiligheid

Principe 8. Beveilig uw mobiele toestellen

Actie 2. Publiceer een eigen veiligheidsbeleid en gedragscode

Actie 11. Beveilig de toegang op afstand

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

5. Heeft uw onderneming een informatieveiligheidsbeleid of richtlijnen voor derden (bijvoorbeeld leveranciers) die toegang hebben tot bepaalde (potentieel) gevoelige informatie?

- (0) Onzeker
- (1) Nee
- (2) Ja, maar het is niet altijd gemakkelijk om het verschil tussen internen en externen te bepalen.
- (3) Ja en de contracten met derden bevatten specifieke clausules, externe leveranciers worden duidelijk als zodanig geïdentificeerd (afzonderlijke badges, afzonderlijke toegang, enz.) en de informatie circuleert uitsluitend in overeenstemming met het classificatiebeleid van de onderneming.

Om verder te gaan:

Onderneming 1.0

Principe 5. Implementeer uw visie

Onderneming 2.0

Principe 10. Werk aan uw relaties met derden

Principe 3. Identificeer de informatie waarover uw bedrijf beschikt en classificeer ze!

6. Geeft uw onderneming richtlijnen aan de werknemers voor de behandeling en "classificatie" van gevoelige informatie?

- (0) Onzeker
- (1) Nee
- (2) Ja, maar deze instructies zijn zo ingewikkeld dat niemand ze toepast.
- (3) Ja en deze instructies worden begrepen en toegepast.

Om verder te gaan:

Onderneming 1.0

Actie 1. Bewaar uw informatie en controleer het herstelproces

Onderneming 2.0

Principe 3. Identificeer de informatie waarover uw bedrijf beschikt en classificeer ze!

7. Beschikt uw onderneming over een bedrijfscontinuïteitsplan (BCP) of een noodherstelplan (DRP) of een incidentbeheerplan?

- (0) Onzeker
- (1) Nee
- (2) Ja, maar niemand kent deze en/of deze procedures zijn nooit getest.
- (3) Ja, het personeel is vertrouwd met deze procedures en er worden regelmatig testen georganiseerd (ten minste eenmaal per jaar).

Om verder te gaan:

Onderneming 1.0

Principe 3. Wees voorbereid om veiligheidsincidenten aan te pakken

Actie 6. Bereid u voor op incidenten

Onderneming 2.0

Principe 7. Werk een realistisch "Incident Management Plan"(IMP) uit

Actie 12. Zorg voor een bedrijfscontinuïteitsplan (BCP) en voor een incidentbeheer-plan

8. Geeft uw onderneming haar werknemers instructies om veilig te werken buiten hun normale werkomgeving (externe vergaderingen, telewerk, ...)?

- (0) Onzeker
- (1) Nee
- (2) Ja, maar er is geen virtueel privénetwerk (VPN)
- (3) Ja en de toegang wordt beschermd door een virtueel privénetwerk (VPN)

Om verder te gaan:

Onderneming 1.0

Actie 4. Houd uw IT-omgeving in de gaten

Onderneming 2.0

Principe 1. Organiseer een "meerlagige" verdediging

Actie 11. Beveilig de toegang op afstand

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

9. Legt uw onderneming een beleid op dat voorziet in een sterke wachtwoordselectie, bewustzijn van wachtwoordbescherming en regelmatige wachtwoordwijzigingen?

- (0) Onzeker
- (1) Nee
- (2) Ja, maar "sterke" wachtwoorden zijn moeilijk te onthouden. Post-its hangen rond, wachtwoorden worden uitgewisseld tussen collega's, dezelfde wachtwoorden worden keer op keer gebruikt, ...
- (3) Ja en iedereen weet hoe een sterk wachtwoord te vormen, waar het veilig kan worden opgeslagen en hoe informatie tussen collega's kan worden uitgewisseld zonder persoonlijke wachtwoorden uit te wisselen.

Om verder te gaan:

Onderneming 1.0

Actie 4. Houd uw IT-omgeving in de gaten

Onderneming 2.0

Actie 8. Beheer de toegang tot uw computers en netwerken

10. Beoordeelt uw onderneming bij de introductie van nieuwe projecten de impact op de informatieveiligheid en de privacy (security/privacy by design en by default)?

- (0) Onzeker
- (1) Nee
- (2) Ja, in principe, maar in de realiteit... is dat een ander verhaal.
- (3) Ja, elke projectmanager weet dat hij dit punt op zijn agenda moet zetten en dat er geen nieuw IT-project kan komen zonder rekening te hebben gehouden met veiligheid en gegevensbescherming.

Om verder te gaan:

Onderneming 1.0

Principe 1. Leg de focus op informatie, niet op de technologie

Onderneming 2.0

Principe 4. Neem maatregelen met betrekking tot de bescherming van de persoonlijke levenssfeer

Actie 3. Maak uw werknemers bewust van de cyberrisico's

Deel B: Technische aspecten

11. Organiseert uw onderneming regelmatig back-ups van al haar servers?

- (0) Onzeker
- (1) Nee
- (2) Ja, maar deze back-ups worden nooit getest en/of bevinden zich direct naast de hoofdservers.
- (3) Ja en deze back-ups worden regelmatig getest (op kwaliteit van de procedures en kwaliteit van de inhoud). Deze back-ups worden bij voorkeur op een andere locatie dan de hoofdlocatie gemaakt.

Om verder te gaan:

Onderneming 1.0

Principe 3. Wees voorbereid om veiligheidsincidenten aan te pakken

Principe 5. Implementeer uw visie

Actie 1. Bewaar uw informatie en controleer het herstelproces

Onderneming 2.0

Principe 1. Organiseer een "meerlagige" verdediging

Principe 7. Werk een realistisch "Incident Management Plan" uit

Actie 12. Zorg voor een bedrijfscontinuïteitsplan (BCP) en voor een incidentbeheer-plan

12. Houdt uw onderneming regelmatig zijn systemen (OS) en applicaties up-to-date?

- (0) Onzeker
- (1) Nee
- (2) Ja, maar niet automatisch. Elk personeelslid moet zijn eigen besturingssysteem en programma's bijwerken. Het is moeilijk om te weten of iedereen dit correct heeft ge-daan.
- (3) Ja. Het besturingssysteem wordt automatisch bijgewerkt en programma's worden beoordeeld en getest na elke wijziging in de besturingssystemen. Beveiligingsback-ups (herstelpunt) worden net daarvoor georganiseerd.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

Om verder te gaan:

Onderneming 1.0

Actie 2. Houd uw IT-systemen steeds up-to-date

Onderneming 2.0

Actie 5. Update alle programma's.

13. Is er een firewall geïnstalleerd tussen uw bedrijfscomputers en het internet?

- (0) Onzeker
- (1) Nee
- (2) Ja, maar niemand weet echt hoe dit werkt.
- (3) Ja en gekwalificeerd personeel (intern of extern) evalueert regelmatig de verslagen en neemt indien nodig maatregelen.

Om verder te gaan:

Onderneming 1.0

Actie 5. Vermenigvuldig de verdediging om risico's te verminderen

Onderneming 2.0

Principe 1. Organiseer een "meerlagige" verdediging

Actie 8. Beheer de toegang tot uw computers en netwerken

14. Beschikt uw onderneming over een tool om spam of phishing te filteren of te blokkeren?

- (0) Onzeker
- (1) Nee
- (2) Ja, maar niemand weet hoe hij een spam- of phishingmail moet herkennen of wat hij moet doen als hij met een dergelijke e-mail te maken krijgt.
- (3) Ja en het personeel is opgeleid om spam/phishing te herkennen en er correct op te reageren.

Om verder te gaan:

Onderneming 1.0

Principe 1. Leg de focus op informatie, niet op de technologie

Onderneming 2.0

Principe 1. Organiseer een "meerlagige" verdediging

Principe 2. Maak uw personeel bewust van informatieveiligheid

Actie 3. Maak uw werknemers bewust van de cyberrisico's

15. Is uw onderneming beschermd tegen kwaadaardige programma's (malware)?

- (0) Onzeker
- (1) Nee
- (2) Ja, maar niet op alle bedrijfscomputers
- (3) Ja, op alle computers worden deze tools regelmatig bijgewerkt.

Om verder te gaan:

Onderneming 1.0

Actie 2. Houd uw IT-systemen steeds up-to-date

Actie 5. Vermenigvuldig de verdediging om risico's te verminderen

Onderneming 2.0

Principe 1. Organiseer een "meerlagige" verdediging

Actie 5. Update alle programma's

Actie 6. Installeer een antivirusbescherming

Actie 9. Beveilig werkposten en mobiele apparaten

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

16. Gebruikt uw onderneming een versleutelingsprogramma (meestal software) om gevoelige informatie te beschermen voordat die buiten de onderneming wordt verzonden (bijvoorbeeld bij het verzenden van bijlagen die vertrouwelijke/gevoelige/persoonsgebonden informatie bevatten)?

- (0) Onzeker
- (1) Nee
- (2) Ja, maar niemand weet hoe men die moet gebruiken
- (3) Ja en het personeel is opgeleid om het te gebruiken.

Om verder te gaan:

Onderneming 1.0

Principe 5. Implementeer uw visie

Actie 1. Bewaar uw informatie en controleer het herstelproces

Actie 4. Houd uw IT-omgeving in de gaten

Onderneming 2.0

Principe 4. Neem maatregelen met betrekking tot de bescherming van de persoonlijke levenssfeer

Actie 7. Maak een back-up van alle informatie

Actie 9. Beveilig werkposten en mobiele apparaten

17. Beschikt uw onderneming over een (efficiënt) datatoegangsbeheer?

- (0) Onzeker
- (1) Nee
- (2) Ja, maar in de praktijk heeft iedereen uiteindelijk toegang tot alles.
- (3) Ja en we hebben een IAM: niet iedereen heeft toegang tot alles.

Om verder te gaan:

Onderneming 1.0

Actie 4. Houd uw IT-omgeving in de gaten

Onderneming 2.0

Actie 8. Beheer de toegang tot uw computers en netwerken

18. Heeft uw onderneming een (permanente) opleiding voor informatie-veiligheidspersoneel opgezet?

- (0) Onzeker
- (1) Nee
- (2) Ja, maar ze zijn alleen intern opgeleid en/of alleen bij aankomst
- (3) Ja en de betrokken personeelsleden krijgen permanente interne en externe opleidingen

Om verder te gaan:

Onderneming 1.0

Actie 3. Investeer in opleidingen

Onderneming 2.0

Principe 2. Maak uw personeel bewust van informatieveiligheid

Principe 10. Werk aan uw relaties met derden

Actie 3. Maak uw werknemers bewust van de cyberrisico's

19. Beveiligt uw onderneming haar servers en netwerkcomponenten op een efficiënte manier?

- (0) Onzeker
- (1) Nee
- (2) Ja, maar de beveiligingslogs op de servers en firewalls worden slechts een maand bewaard en niemand heeft tijd om ze goed te analyseren.
- (3) Ja en beveiligingslogs op servers en firewalls worden minstens 6 maanden bewaard. Een analyse- en waarschuwingssysteem (SIEM) onderzoekt deze logboeken ook om kwaadaardig gedrag op te sporen.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

Om verder te gaan:

Onderneming 1.0

Actie 4. Houd uw IT-omgeving in de gaten

Onderneming 2.0

Principe 10. Werk aan uw relaties met derden

Actie 4. Beheer uw belangrijke ICT-onderdelen

Actie 5. Update alle programma's

Actie 8. Beheer de toegang tot uw computers en netwerken

Actie 10. Beveilig servers en netwerkcomponenten

Actie 11. Beveilig de toegang op afstand

20. Wordt de informatiebeveiliging regelmatig geëvalueerd in uw onderneming (security audit)?

- (0) Onzeker
- (1) Nee
- (2) Ja, maar er wordt niets gevraagd aan de leveranciers en niemand evalueert intern het nut van de informatie die de audit heeft voortgebracht.
- (3) Ja en ook het nut van de verzamelde informatie wordt beoordeeld of het nu een interne audit betreft of een audit uitgevoerd bij de leverancier.

Om verder te gaan:

Onderneming 1.0

Principe 4. Laat zien dat u verantwoordelijkheid neemt

Principe 5. Implementeer uw visie

Onderneming 2.0

Principe 5. Organiseer regelmatig tests en controles

Principe 10. Werk aan uw relaties met derden

Actie 4. Beheer uw belangrijke ICT-onderdelen

Actie 8. Beheer de toegang tot uw computers en netwerken