



CYBERFUNDAMENTALS BASIC VOOR LEVERANCIERS

Wat ontbreekt er bij vdhSchrijnwerk voor CyberFundamentals Basic?

Zelfevaluatie, gaplijst en stappenplan voor een leverancier die het niveau van een klant opgelegd krijgt

vdhSchrijnwerk BV, Herent (18 medewerkers, één vestiging)
Opgesteld op 20 oktober 2026

VOORBEELDUITTREKSEL - vdhSchrijnwerk BV is een fictief bedrijf

Basic is haalbaar in 6 tot 10 weken. Van de 34 maatregelen van het Basic-niveau zijn er 20 in orde, 9 deels en 5 niet. De twee grootste gaten: back-ups die met het netwerk verbonden blijven, en toegang op afstand met alleen een wachtwoord. Beide zijn met de bestaande IT-partner op te lossen, samen ongeveer 2 tot 3 dagen werk.

Inhoud van het volledige rapport

In het kort (in dit uittreksel)	2
1. Vraag van de klant en afbakening	3
2. Zelfevaluatie per functie (Identificeren tot Herstellen)	4
3. Gaplijst in gewone taal	7
3.1 Back-ups (in dit uittreksel)	7
3.2 Toegang op afstand (in dit uittreksel)	8
4. Stappenplan met prioriteit, kost en tijd	10
5. Samenvatting voor uw klant	12
Bijlage. Ingevulde zelfevaluatie (Excel van het CCB)	13

Het volledige rapport telt 14 pagina's. Dit uittreksel toont de samenvatting en twee bevindingen; de werkwijze, de volledige lijsten en de bijlagen staan alleen in het rapport voor de klant.

Dit is een voorbeelduittreksel. vdhSchrijnwerk BV, haar IT-omgeving en de cijfers zijn verzonnen. De maatregelen verwijzen naar het CyberFundamentals-kader van het Centrum voor Cybersecurity België (CCB). De verificatie door een geaccrediteerde instantie valt buiten de opdracht.

In het kort

Een klant van vdhSchrijnwerk, zelf een belangrijke entiteit onder de NIS2-wet, vraagt in zijn leveranciersvoorwaarden CyberFundamentals Basic tegen 1 juni 2027. Ik vulde de zelfevaluatie in met de zaakvoerder en de externe IT-partner (twee gesprekken van een uur). Hieronder twee punten uit de gaplijst.

De back-up staat op een NAS die altijd aan het netwerk hangt

Hoog | Wie: IT-partner | Tijd: 1 tot 2 dagen, plus EUR 15 tot 40 per maand opslag

Wat ik zag. De dagelijkse back-up van de server en de boekhouding gaat naar een NAS in het bureau, met een netwerkschijf die elke pc kan beschrijven. Er is geen kopie buiten het gebouw en geen offline kopie. Een terugzetting is nooit getest.

Waarom het telt. Gijzelsoftware versleutelt alles wat een besmette pc kan bereiken, ook een verbonden back-up. Dan is er niets om terug te zetten. Basic vraagt een back-up op een ander systeem dan de originele gegevens; dat is hier zo, maar die kopie overleeft gijzelsoftware niet. Een geteste back-up op een aparte opslagplaats is een maatregel van het niveau Important; voor een klant die zekerheid wil, is het de goedkoopste verbetering.

Wat te doen. Een tweede kopie die niet vanaf de werkposten te beschrijven is (een onveranderbare cloudopslag of een schijf die wekelijks wordt losgekoppeld), en een terugzetest per kwartaal met een kort verslag. Dat verslag is meteen het bewijs voor de zelfevaluatie.

Bron. CyberFundamentals Framework van het CCB, niveau Basic, functie Beschermen, maatregelen over back-ups (PR.DS-11.1 op Basic; PR.DS-11.2 en PR.DS-11.3 op Important; CyFun 2025). Gelezen op 20 oktober 2026.

Toegang op afstand gebeurt met alleen een wachtwoord

Hoog | Wie: IT-partner, zaakvoerder beslist | Tijd: een halve dag

Wat ik zag. De zaakvoerder en twee werfleidings werken van thuis via een extern bureaublad, met een gebruikersnaam en een wachtwoord. Er is geen tweede factor. Het mailaccount van de zaakvoerder heeft ook geen tweede factor.

Waarom het telt. Een gelekt of geraden wachtwoord geeft dan rechtstreeks toegang tot het netwerk. Basic eist tweestapsverificatie voor toegang op afstand tot het netwerk, en het is het eerste wat een klant navraagt.

Wat te doen. Tweestapsverificatie aanzetten voor de toegang op afstand en voor alle mailaccounts, te beginnen bij de zaakvoerder en de boekhouding. De IT-partner kan dat meestal binnen de bestaande licenties. Staat het extern bureaublad rechtstreeks open op het internet, dan hoort het achter een VPN of een gateway met tweestapsverificatie.

Bron. CyberFundamentals Framework van het CCB, niveau Basic, functie Beschermen, maatregel over tweestapsverificatie bij toegang op afstand (PR.AA-03.2, CyFun 2025). Gelezen op 20 oktober 2026.