

Zo werkt de CyberCheck-scan in de praktijk

De digitale weerbaarheid van het mkb staat steeds vaker onder druk. Daarom is er de **CyberCheck-scan**: een initiatief waarbij studenten samen met ondernemers werken aan praktische oplossingen voor digitale veiligheid.

Dit is deel 2 van een serie van drie artikelen over de achtergrond, uitvoering en toekomst van deze aanpak. Lees deel 1 voor informatie over de achtergrond en opzet van de CyberCheck-scan. In deel 3 kijken we vooruit naar de toekomst en opschaling.

Laagdrempelig en gestructureerd

Een CyberCheck-scan duurt gemiddeld één uur en kan op locatie of online worden uitgevoerd. Het traject is laagdrempelig opgezet, met duidelijke stappen, vaste begeleiders en een heldere uitkomst. Studenten van Hogeschool Saxion en Aventus voeren de scan uit onder begeleiding van docenten en professionals vanuit de Digitale Werkplaats of het Centrum voor Veiligheid en Digitalisering.

“We zorgen dat studenten goed voorbereid zijn en altijd werken onder begeleiding. Zo waarborgen we kwaliteit en vertrouwen,” zegt Stefan van Malsen, coördinator CyberCheck-scans.

Hoe verloopt een CyberCheck-scan precies?

De CyberCheck-scan is een laagdrempelig en praktisch traject dat gemiddeld één uur in beslag neemt. Tijdens dit uur doorlopen studenten samen met de ondernemer vier fasen. Het begint met een korte kennismaking: de studenten stellen zich voor en geven uitleg over het doel en de opzet van de scan. De ondernemer schetst op zijn of haar beurt de bedrijfscontext, zodat de studenten inzicht krijgen in de organisatie en de digitale werkomgeving.

Daarna volgt de interview- en inventarisatiefase. Aan de hand van een gestructureerde vragenlijst — gebaseerd op de vijf basisprincipes van het Digital Trust Center (DTC) — bespreken studenten en ondernemer onderwerpen als wachtwoordgebruik, back-upvoorzieningen, software-updates en toegangsbeheer. Ook het bewustzijn van medewerkers over digitale veiligheid komt aan bod.



Centrum voor
Veiligheid en
Digitalisering



In de derde fase analyseren de studenten de verzamelde informatie en stellen zij een adviesrapport op. Dit rapport bevat concrete verbeterpunten die de ondernemer direct kan toepassen, met nadruk op eenvoud, haalbaarheid en effect.

Tot slot is er ruimte voor nazorg. Soms volgt een vervolgggesprek om dieper in te gaan op specifieke aanbevelingen of wordt de ondernemer doorverwezen naar een specialist voor verdere ondersteuning.

Door deze gestructureerde aanpak, en dankzij de begeleiding van docenten en professionals, krijgen zowel studenten als ondernemers veel waarde uit het traject — met praktische resultaten op korte én lange termijn.

Vertrouwelijkheid en gegevensbescherming

Om de vertrouwelijkheid van de gedeelde informatie tijdens een CyberCheck-scan te waarborgen, zijn verschillende maatregelen getroffen. Het basisrapport wordt na afloop automatisch gegenereerd via het Digital Trust Center (DTC) en rechtstreeks per e-mail naar de ondernemer verzonden, zonder tussenkomst van derden. Wanneer studenten een verdiepende analyse opstellen, gebeurt dit onder strikte begeleiding en binnen de privacyrichtlijnen van hun onderwijsinstelling. De uitkomsten van scans worden nooit extern verspreid en blijven uitsluitend beschikbaar voor het bedrijf in kwestie.

Bovendien is het hele programma ingebed in een netwerk van betrouwbare partners — waaronder Saxion, Aventus, de Digitale Werkplaats, het Centrum voor Veiligheid en Digitalisering en het DTC — die structureel toezien op informatiebeveiliging. Deze aanpak geeft ondernemers het vertrouwen om open te spreken over hun digitale kwetsbaarheden, en helpt hen om in een veilige setting gerichte stappen te zetten naar een weerbaarder bedrijfsvoering.

Hoe cyberweerbaar is jouw organisatie?

Ontdek het met de gratis CyberCheck-scan. [Vul het aanmeldformulier in op cvdonderland.nl/check](https://cvdonderland.nl/check) en krijg inzicht in jouw kwetsbaarheden en verbeterpunten!