avit part of springboardnetwork | Tabor College



Van nulmeting naar roadmap: Cyberweerbaarheid in het voortgezet onderwijs



Informatiebeveiliging in het onderwijs is een uitdaging. Beperkte budgetten, personeelstekorten en steeds strengere wet- en regelgeving maken het lastig om grip te krijgen op cybersecurity. Toch is het noodzakelijk: cyberaanvallen op scholen krijgen steeds meer aandacht en de impact kan enorm zijn.

Het Tabor College in Hoorn zocht naar een manier om objectief te meten waar ze stonden op het gebied van informatiebeveiliging.

Oscar Cohen, Hoofd ICT en Privacy Officer, wilde niet alleen weten óf ze voldoende beveiligd waren, maar vooral ook welke concrete stappen nodig waren om de beveiliging verder te professionaliseren.



In deze case lees je hoe Avit het Tabor College heeft geholpen met een Cyber Resilience Assessment op basis van de CIS Controls. Van nulmeting tot werkbare roadmap, met praktische inzichten en organisatiebreed draagvlak.

Organisatie:	Tabor College, Hoorn
Sector:	Voortgezet Onderwijs
Omvang:	3.500 leerlingen, verdeeld over 3 schoollocaties, en een bestuursbureau
IT-omgeving:	Volledig Apple-ecosysteem met iPads voor leerlingen en MacBooks voor medewerkers

DE UITDAGING

Het Tabor College kampte met een herkenbaar probleem in het onderwijs: hoe krijg je grip op informatiebeveiliging met personeelstekorten, beperkte budgetten én steeds strengere wet- en regelgeving?

Het IBP-normenkader voor onderwijs vraagt naleving van **94** normen verdeeld over informatiebeveiliging en privacy. Daarnaast komt de NIS2-wetgeving eraan, met implementatie gepland voor het tweede kwartaal van 2026.

Ook speelde de vraag: hoe voorkom je dat je als school een van de voorbeelden in het nieuws wordt? Cyberaanvallen op onderwijsinstellingen krijgen steeds meer aandacht en de impact kan enorm zijn. Een objectieve nulmeting was dus hard nodig.

Oscar Cohen is verantwoordelijk voor de gehele IT-infrastructuur en informatiebeveiliging van het Tabor College. Als Privacy Officer houdt hij zich ook bezig met AVG-naleving en de implementatie van het IBP-normenkader voor onderwijs. Met een pragmatische aanpak zoekt hij naar concrete oplossingen die passen bij de middelen en mogelijkheden van een onderwijsinstelling.



Oscar: "Je wil op een gegeven moment ook een beetje zien waar je staat. We hadden zelf al een tool waarin we alle beleidsstukken hadden gezet, maar we wilden graag dat iemand van buitenaf kwam kijken: Hé, hoe staan jullie ervoor? Zodat je ook echt een meetpunt hebt."

DE OPLOSSING

Cyber Resilience Assessment

Avit voerde een Cyber Resilience Assessment uit op basis van de CIS Controls (Center for Internet Security). Het assessment bestond uit een intensieve workshop van 8 uur waarin we alle 153 controles verdeeld over 18 domeinen doorliepen.

Interactieve samenwerking

Het bijzondere aan deze aanpak is de interactieve manier van werken. Per control werd gezamenlijk bepaald in hoeverre deze geïmplementeerd was. Soms zaten de meningen uit elkaar, maar juist die discussies zorgden voor waardevolle inzichten.

De bevindingen werden niet alleen afgezet tegen wereldwijde benchmarks binnen het onderwijssegment, maar ook specifiek getoetst aan de **NIS2-vereisten**.

Van analyse naar draagvlak

Na de workshop volgde een grondige analyse waarbij alle bevindingen per domein in kaart werden gebracht. Het conceptrapport werd besproken in een eindpresentatie met alle relevante stakeholders, waaronder de bestuurder. Dit zorgde ervoor dat het eindrapport volledig aansloot bij de praktijk én door iedereen gedragen werd.



RESULTATEN

Van inzicht naar actie

Het assessment leverde meer op dan alleen een rapport. Het Tabor College kreeg een helder, objectief beeld van waar ze stonden. Wat ze al goed deden werd bevestigd, maar ook blinde vlekken kwamen aan het licht.

Een belangrijke ontdekking was bijvoorbeeld het ontbreken van een PDCA-cyclus [SvdB1.1] voor documentatie. Ondanks goed lifecycle management op technisch gebied, ontbrak de beleidsmatige borging. Precies dit soort praktische inzichten maken het verschil.

Een werkbare roadmap

De roadmap die uit het assessment voortkwam is geen compleet vaststaand plan. Het bestaat uit behapbare blokken die flexibel ingepland kunnen worden, afhankelijk van beschikbare tijd en middelen.

Het assessment leverde concrete handvatten:

- Quick wins die weinig kosten maar veel effect hebben
- Grotere verbetertrajecten die nu goed onderbouwd kunnen worden richting het bestuur
- Objectieve benchmarks om voortgang te meten
- Een roadmap die aansluit bij de realiteit van het onderwijs: beperkte middelen, maar wel structurele verbetering

Oscar Cohen vat het samen: "Het geeft heel duidelijk weer waar je staat, wat je nog moet doen, maar ook wat je nog niet doet zoals het zou moeten. Het levert je heel veel inzichten op, bruikbare inzichten, die je heel goed kunt gebruiken binnen het onderwijs, maar dat geldt natuurlijk ook voor bedrijven."

Meer dan een rapport: Teambuilding en draagvlak

Een onverwachte maar waardevolle bijkomstigheid was het effect op de samenwerking binnen de organisatie. Door een hele dag gezamenlijk alle controles door te nemen, ontstond er begrip voor elkaars werk en uitdagingen. De neuzen kwamen dezelfde kant op te staan. Informatiebeveiliging is niet alleen een ICT-aangelegenheid, maar vraagt om inzet van de hele organisatie.

Ook het management raakte meer betrokken, de uitkomst sloot aan bij wat iedereen al vermoedde, maar het Tabor College kreeg nu concrete handvatten om vervolgstappen te ondersteunen.

CIS Controls: De kracht van concrete handvatten

Waarom werkt het assessment op basis van CIS Controls zo goed?

Het framework vult bestaande normenkaders als ISO 27001 en het IBP-normenkader aan door zeer concrete, technische implementatie-richtlijnen te geven. Waar ISO bijvoorbeeld stelt dat een organisatie procedures moet opstellen voor patch management, specificeert CIS Controls dat je automatische kwetsbaarheidsscans minimaal wekelijks moet uitvoeren en patches binnen 30 dagen moet implementeren.

Deze concreetheid maakt het voor IT-teams direct werkbaar. Je weet precies wat er van je verwacht wordt en hoe je invulling kunt geven aan de meer beleidsmatige eisen uit andere normenkaders.



Extra relevant voor het onderwijs

Bij volledige compliance met het IBP-normenkader ben je automatisch NIS2-compliant. Dat scheelt dubbel werk en maakt de investering nog waardevoller.

Een roadmap als solide basis

Het Cyber Resilience Assessment heeft het Tabor College een solide basis gegeven voor verdere professionalisering van hun informatiebeveiliging. Geen dik boekwerk dat in de kast verdwijnt, maar een praktische roadmap met quick wins én strategische vervolgstappen.

De combinatie van objectieve beoordeling, benchmarking en organisatiebrede betrokkenheid heeft gezorgd voor draagvlak en concrete verbeteringen.

Voor Oscar Cohen en zijn team is het assessment het startpunt geweest van een duurzaam verbetertraject. Met beperkte middelen en capaciteit werken ze stap voor stap aan een beter beveiligde digitale omgeving, terwijl ze voldoen aan wet- en regelgeving.

En misschien wel het belangrijkste: ze weten waar ze staan en waar ze naartoe gaan.

avit
part of springboardnetwork

Over Avit en het Cyber Resilience Assessment

Avit ondersteunt organisaties bij het verbeteren van hun cyberweerbaarheid door middel van Cyber Resilience Assessments op basis van de CIS Controls. Met een pragmatische aanpak en ervaren consultants helpen we organisaties om informatiebeveiliging naar een hoger niveau te tillen, zonder dat het een papieren tijger wordt.

Meer weten?

Bekijk onze keynote over het Cyber Resilience Assessment of neem contact op voor een vrijblijvend gesprek:

info@avitgroup.com
088 - 0321032