

Et dybt dyk ned i cybersikkerhed: støtte til skolars databeskyttelse og dataejerskab

RESUMÉ

30 June 2025

Problem og kontekst

I takt med at nederlandske skoler i stigende grad benytter digitale læringsværktøjer og EdTech-tjenester, er databeskyttelse og cybersikkerhed blevet et vigtigt emne. Skolerne mangler imidlertid ofte den ekspertise, den tid eller de standardiserede processer, der er nødvendige for effektivt at håndtere disse risici. Et decentraliseret uddannelsessystem, hvor skolebestyrelser handler uafhængigt, forværrer dette problem ved at skabe forskelle i den digitale sikkerhed blandt institutionerne.

Som reaktion herpå iværksatte SIVON med støtte fra Kennisnet og det nederlandske undervisningsministerium en række nationale tiltag til styrkelse af datastyring og cybersikkerhed i grundskolen. Et af disse initiativer, Deep Dive-projektet, blev lanceret for at vurdere de nuværende digitale sikkerhedspraksisser og hjælpe skolerne med at udarbejde skræddersyede planer for forbedring.

Deep Dive-projektet

Deep Dive-projektet, der blev gennemført af SIVON, evaluerede informationsikkerhedens modenhedsniveau for 15 skolebestyrelser (der repræsenterer 290 skoler og 80.000 elever) ved hjælp af en nyudviklet [ramme for standarder](#), der består af 69 benchmarks på tværs af 15 domæner (f.eks. risikostyring, sikkerhedspolitik, hændeshåndtering). De vigtigste skridt omfattede:

1. **Udgangsvurdering.** Certificerede auditorer brugte to dage på at evaluere hver skolebestyrelses infrastruktur for databeskyttelse og vurderede dem på en skala fra 1 til 4. Skolerne scorede mellem 1,3 og 2,5, hvilket indikerer store forskelle mellem skolerne.
2. **Skræddersyede planer for forbedring.** Resultaterne blev drøftet med de relevante interessenter (skoleledere, it-medarbejdere, HR), og der blev fremsat skræddersyede anbefalinger. Skolerne modtog en risikovurdering og forpligtede sig til at iværksætte specifikke tiltag baseret på deres behov og modenhedsniveau.
3. **Oplæring og kapacitetsopbygning.** Skolerne opfordredes til at oplære deres medarbejdere, definere roller inden for digital sikkerhed, visualisere ikt-miljøer og udvikle politikker for mail- og filopbevaringsprotokoller.
4. **Eksempel fra casestudiet – De Rank.** Denne grundskole samarbejdede med SIVON om at udvikle en handlingsplan for datasikkerhed, fremme ikt-oplæring og forbedre kortlægningen af den digitale infrastruktur og ansvarsfordeling.

Ud over Deep Dive havde SIVON og Kennisnet også en **omfattende pakke af tjenester** til forbedring af den digitale sikkerhed på hele skolen.

- **Storindkøb** af EdTech-værktøjer, -tjenester og -infrastruktur til nedsat pris. Dette medvirkede f.eks. til, at priserne kunne forhandles ned - i ét tilfælde helt ned til en prisnedsættelse på 40 % for interaktive whiteboards.
- **Skabelon til databeskyttelsesaftaler** for at strømline overholdelse af lovgivningen.
- **Akutberedskab** til malware- eller ransomware-hændelser.
- **Professionelle netværk** som f.eks. det 900 medlemmer store »Network IBP« til at dele erfaringer.
- **Tjenester til risikoanalyse** og praktiske retningslinjer for implementering af cybersikkerhedspolitikker.

Sideløbende hermed førte **landsdækkende forhandlinger med tech-giganter (f.eks. Google, Microsoft, Apple)** til vigtige fremskridt, såsom garantier for dataejerskab og begrænsninger i kommerciel brug af data. Disse forhandlinger var baseret på **konsekvensanalyser (DPIAs)** gennemført af SIVON.

Erfaringer

- Områder som organisation, risikostyring og systemudvikling var generelt svage. Et almindeligt problem er, at skolerne ikke har en krisehåndteringsplan og solide procedurer for sikkerhedskopiering af data. De har heller ingen beskrivelser af opgaver vedrørende datasikkerhed. Ved første øjekast er de mest almindelige behov på skolerne at øge viden om datasikkerhed, centralisere administrationen af software-as-a-service-leverandører og indføre flere retningslinjer.
- Skolerne er mere modne med hensyn til håndtering af hændelser, fordi mange skolebestyrelser outsourcer deres databeskyttelsesprocesser til professionelle tjenesteudbydere.
- De fleste skoler opfyldte ikke de grundlæggende standarder. Især mindre skoler havde svært ved at leve op til standarderne på grund af begrænset kapacitet.
- Skoler har en tendens til at prioritere værktøjernes funktionalitet højere end databeskyttelse, som f.eks. hvordan personoplysninger gemmes eller behandles.
- Skolerne anmodede SIVON om at bruge et tydeligere sprog og mere relevante benchmarks, især til de skoler, der ikke udvikler deres egen software. Der blev også foreslået en centraliseret risikostyring af leverandører som en mere gennemførlig løsning end på bestyrelsesniveau.
- Tillidsbaserede offline netværksarrangementer kan fremme gennemsigtighed for skoler med et lavere modenhedsniveau og skabe en produktiv udveksling af bedste praksis.

- Den første stikprøve var skæv, da der var en overvægt af skoler, der allerede var interesseret i, eller allerede arbejdede med digital sikkerhed. Ikke desto mindre gjorde de medvirkende 290 skoler dette til et stort og informativt pilotprojekt for SIVON.

Ved at kombinere regulatoriske rammer, praktiske værktøjer, centraliserede forhandlinger og støtte på skoleniveau viser denne nederlandske model, hvordan uddannelsessystemer kan tage meningsfulde skridt for at beskytte skoledata og indgå indkøbsaftaler, der er mere fordelagtige for skolerne.

Selvom de indledende evalueringer viste, at der var god plads til forbedringer, banede struktureret vejledning, kapacitetsopbygning og inddragelse af interessenter vejen for langsigtet digital sikkerhed. Det endelige mål er at bringe alle skoler op til standarden inden 2027 inden for en lovramme, der i øjeblikket er under udarbejdelse af Undervisningsministeriet. Denne historie tjener som et eksempel på koordinering på nationalt niveau, forhandlingsstyrke i den offentlige sektor og implementeringsstøtte nedefra.



Medfinansieret af
Den Europæiske Union

Finansieret af Den Europæiske Union. Synspunkter og holdninger, der kommer til udtryk, er udelukkende forfatterens/forfatternes og er ikke nødvendigvis udtryk for Den Europæiske Unions eller Det Europæiske Forvaltningsorgan for Uddannelse og Kulturs (EACEA) officielle holdning. Hverken den Europæiske Union eller EACEA kan holdes ansvarlig herfor.