

# Djupdykning i cybersäkerhet: att stödja skolors datasäkerhet och äganderätt

SAMMANFATTNING

30 June 2025

## Problematisering och kontext

I takt med att nederländska skolor blir allt mer beroende av digitala lärverktyg och Edtech-tjänster (Educational Technology) har datasäkerhet och cybersäkerhet blivit viktiga frågor. Skolor saknar dock ofta den expertis, tid eller standardiserade processer som krävs för att hantera dessa risker på ett effektivt sätt. Ett decentraliserat utbildningssystem, där skolledningar agerar självständigt, förvärrar problemet genom att skapa skillnader i digital säkerhet mellan olika institutioner.

Som svar på detta initierade SIVON, med stöd av Kennisnet och det nederländska utbildningsdepartementet, en rad nationella åtgärder för att stärka datastyrningen och cybersäkerheten inom grundskolan och gymnasiet. Ett sådant initiativ, Deep Dive-projektet, lanserades för att utvärdera nuvarande digitala säkerhetsrutiner och hjälpa skolor att ta fram skräddarsydda planer för förbättring.

## Deep Dive-projektet

Deep Dive-projektet, som genomfördes av SIVON, utvärderade mognadsgraden inom informationssäkerhet hos 15 skolstyrelser (som representerar 290 skolor och 80 000 elever) med hjälp av ett nyutvecklat [Ramverk med standardiserade riktlinjer](#) som omfattar 69 riktmärken inom 15 områden (t.ex. riskhantering, säkerhetspolicy och incidenthantering). De viktigaste stegen omfattade:

1. **Baslinjebedömning.** Certifierade revisorer tillbringade två dagar med att utvärdera varje skolstyrelses infrastruktur för datasäkerhet och betygsatte dem på en skala från 1 till 4. Skolorna fick poäng mellan 1.3 och 2.5, vilket visar på stora skillnader mellan skolorna.
2. **Skräddarsydda förbättringsplaner.** Resultaten diskuterades med berörda aktörer (skolledare, IT-personal, HR) och skräddarsydda rekommendationer lämnades. Skolorna fick en sammanfattning av riskerna och åtog sig att vidta specifika åtgärder utifrån behov och mognadsgrad.
3. **Utbildning och uppbyggnad av olika kompetenser.** Skolorna uppmuntrades att utbilda personal, definiera ansvarsområden inom digital säkerhet, visualisera IKT-miljöer och utveckla riktlinjer för e-post och protokoll för lagring av filer.
4. **Fallstudie – De Rank.** Den här grundskolan samarbetade med SIVON för att ta fram en handlingsplan för datasäkerhet, främja IKT-utbildning och förbättra kartläggningen av den digitala infrastrukturen och ansvarsfördelningen.

Utöver Deep Dive tillhandahöll SIVON och Kennisnet en **omfattande uppsättning tjänster** för att förbättra den digitala säkerheten i hela skolan.

- **Volyminköp** av Edtech-verktyg, tjänster och infrastruktur till reducerade kostnader. Detta hjälpte till exempel vid prisförhandlingar, i ett fall till en sänkning på 40% för interaktiva skrivtavlor.
- **Modellavtal** om integritetsskydd för att effektivisera efterlevnaden av lagar och regler.
- **Akutinsatser** vid incidenter med skadlig programvara eller krypteringsprogram.
- **Professionella nätverk** som det 900 medlemmar starka "Network IBP" för att dela erfarenheter.
- **Risikanalystjänster** och praktiska riktlinjer för genomförande av strategier för cybersäkerhet.

Parallellt med detta har **landsomfattande förhandlingar med teknikjättar (t.ex. Google, Microsoft och Apple)** lett till viktiga framsteg, bland annat garantier för äganderätten till data och begränsningar av kommersiell användning av data. Dessa förhandlingar baserades på **konsekvensbedömningar avseende dataskydd (DPIA)** som leddes av SIVON.

## Lärdomar

- Organisation, riskhantering och systemutveckling var genomgående svaga områden. Ett vanligt problem är att skolor saknar krishanteringsplan och effektiva rutiner för säkerhetskopiering av data. De har inte heller några beskrivningar av arbetsuppgifter som rör datasäkerhet. Vid en första anblick är skolornas vanligaste behov att öka kunskapen om datasäkerhet, centralisera hanteringen av leverantörer av programvara som tjänst och få fler riktlinjer.
- Skolor är mer rutinerade när det gäller incidenthantering, eftersom många skolstyrelser lägger ut sina processer för dataskydd på professionella leverantörer av tjänster.
- De flesta skolor uppfyllde inte minimikraven. Särskilt mindre skolor hade svårt på grund av begränsad kompetens.
- Skolor har en tendens att prioritera verktygens funktionalitet framför integritetsskydd, till exempel hur personuppgifter lagras eller behandlas.
- Skolorna efterfrågade tydligare språk och mer relevanta riktmärken från SIVON, särskilt för dem som inte utvecklar egen programvara. Centraliserad riskhantering av leverantörer föreslogs också som mer rimligt än insatser på ledningsnivå.
- Förtroendebaserade event för nätverkande som inte sker online kan uppmuntra mindre erfarna skolor att vara transparenta och främja ett produktivt utbyte av bästa praxis.
- Det inledande urvalet var snedfördelat mot skolor som redan var intresserade av eller arbetade med digital säkerhet. Trots detta var det ett mycket omfattande och informativt pilotprojekt för SIVON eftersom det innefattade 290 skolor.

Genom att kombinera regelverk, praktiska verktyg, centraliserade förhandlingar och stöd på skolnivå visar den nederländska modellen hur utbildningssystem kan vidta meningsfulla åtgärder för att skydda skolors data och ingå inköpsavtal som är mer fördelaktiga för skolorna.

Även om de inledande utvärderingarna visade på betydande förbättringsmöjligheter, har den strukturerade vägledningen, uppbyggnaden av olika kompetenser och aktörernas engagemang lagt grunden för en långsiktig utveckling av den digitala säkerheten. Slutmålet är att alla skolor ska uppfylla kraven senast 2027, inom ramen för ett rättsligt ramverk som för närvarande utarbetas av utbildningsdepartementet. Denna berättelse fungerar som en modell för samordning på nationell nivå, förhandlingsstyrka inom den offentliga sektorn och stöd för genomförande från gräsrotsnivå.



Medfinansieras av  
Europeiska unionen

Finansieras av Europeiska unionen. De synpunkter och åsikter som uttrycks är endast upphovsmannens [upphovsmännens] och utgör inte Europeiska unionens eller Europeiska genomförandeorganet för utbildning och kulturs (EACEA) officiella ståndpunkt. Varken Europeiska unionen eller EACEA tar något ansvar för dessa.