Inspectie van het Onderwijs
Ministerie van Onderwijs, Cultuur
en Wetenschap

Digitale weerbaarheid en veiligheid in jaarverslagen

Monitor digitale weerbaarheid en veiligheid 2025

Mei 2026

Op welke manier rapporteren schoolbesturen in het onderwijs over de kwaliteitszorg rondom digitale weerbaarheid en veiligheid? En hoe uitgebreid doen ze dat? Daarover gaat deze herhaalde monitor. Vanaf 2024 zijn besturen in het funderend onderwijs namelijk verplicht om informatiebeveiliging en privacy in hun jaarverslag op te nemen. In deze uitgave leest u hoe besturen in alle sectoren zich hierover verantwoorden. En wat de gevolgen zijn van de nieuwe Cyberbeveiligingswet voor het hoger onderwijs.

Voorwoord

Digitale dreigingen komen steeds vaker voor, ook in het onderwijs. Een cyberincident kan meteen grote gevolgen hebben voor leerlingen, studenten, hun ouders en medewerkers van de school. Daarom is het zo belangrijk dat besturen structureel tijd en middelen beschikbaar stellen om te waarborgen dat het onderwijs dag in dag uit door kan gaan. Dat er geen discussie of twijfel is over de kwaliteit van diploma's. En dat de juiste mensen zeker weten dat zij over correcte, betrouwbare gegevens beschikken. Uit onderzoek naar digitale weerbaarheid blijkt dat veel besturen aandacht hebben voor dit thema.

Toch is er nog veel te winnen, blijkt uit deze monitor. Dat vind ik ronduit zorgelijk. Daarom wil ik hen dringend oproepen: zorg dat je je als bestuur goed voorbereidt op digitale dreigingen. Want de vraag is niet óf je met een cyberincident te maken krijgt, maar wannéér. En deel vooral je kennis en ervaringen binnen het onderwijs. Met zo'n aanpak draag je als bestuur bij aan de digitale weerbaarheid en veiligheid van het héle onderwijsveld.

Alida Oppers
inspecteur-generaal van het Onderwijs

Samenvatting

- **Forse toename verantwoording** – in 2023 rapporteert 74% van de besturen in het jaarverslag over digitale weerbaarheid en veiligheid. In 2024 is dit 94%.
- **Deel besturen legt geen verantwoording af** – dit betekent ook dat 6% van de besturen hierover nog niet rapporteert.
- **Verschuiving van privacy naar cybersecurity** – in 2021 gaat 46% van de onderzochte passages over privacy en 28% over cybersecurity. In 2024 is dit 26% privacy en 50% cybersecurity.
- **Geen verandering inhoud verantwoording** – over 2021 tot en met 2024 beschrijft gemiddeld 12% van de passages uitsluitend digitale risico's. 64% bevat maatregelen die besturen nemen. En 6% bevat een evaluatie. In deze laatste passages ziet de inspectie delen van de planning-en-controlcyclus terug. De overige passages bieden onvoldoende informatie om ze te kunnen typeren.
- **Digitale dreigingen aanpakken is een gezamenlijke taak** voor iedereen binnen onderwijsinstellingen, partners in de keten, het gehele onderwijsveld én de inspectie.

Aanleiding

Het onderwijs is afhankelijk van digitale systemen, maar nog niet altijd goed voorbereid op digitale dreigingen

Veel bedrijven en organisaties zijn afhankelijk van een heleboel verschillende informatietechnologieën (IT). Ook in het onderwijs biedt IT allerlei toepassingen. Leerlingen en studenten gebruiken bijvoorbeeld tools om presentaties te ondersteunen. Leraren en docenten leggen de voortgang vast in digitale dossiers. Ouders en begeleiders kunnen vanuit hun eigen omgeving die voortgang inzien. Stafmedewerkers voeren administratie in gespecialiseerde systemen in. Tal van boeken en leermiddelen zijn alleen nog via een digitale omgeving bereikbaar. Toetsen en examens kunnen online gemaakt worden. En de Covid-pandemie heeft de mogelijkheden van afstandsonderwijs en thuiswerken versneld. Zo zijn er nog veel meer voorbeelden te geven. Maar aan alle IT-gerelateerde zaken kleven ook risico's. Als een risico of verstoring zich voordoet, kan dit niet alleen gevolgen hebben voor de continuïteit van het onderwijs en de kwaliteit van diplomering. Maar ook voor de veiligheid en betrouwbaarheid van gegevens en de rechtmatige besteding van de bekostiging. Om die reden vindt de inspectie digitale weerbaarheid en veiligheid in het onderwijs belangrijk. Besturen van onderwijsinstellingen moeten structureel investeren in de digitale weerbaarheid en veiligheid van de organisatie. Dat kunnen ze doen via maatregelen om systemen en data te beschermen tegen ongeautoriseerde toegang en fouten te voorkomen. Ook moet het bestuur een crisisplan hebben voor die momenten dat een cyberincident plaatsvindt. Het delen van kennis en ervaringen helpt vervolgens andere bestuurders weer om de maatregelen gericht aan te scherpen. Hierdoor werken we met elkaar aan digitale weerbaarheid en veiligheid van het onderwijs.

Digitale weerbaarheid en veiligheid
Digitale veiligheid gaat over de feitelijke bescherming van systemen, gegevens en gebruikers tegen digitale dreigingen, zoals hackpogingen of datalekken.
Digitale weerbaarheid gaat een stap verder: het vermogen om die veiligheid structureel te borgen, incidenten tijdig te ontdekken, schade te beperken en snel te herstellen.

Vanaf 2024 geldt ook een verantwoordingsverplichting voor het funderend onderwijs

Beleid op informatiebeveiliging en privacy is een onmisbare stap naar digitale weerbaarheid en veiligheid. Besturen in het funderend onderwijs zijn vanaf verslagjaar 2024 verplicht om informatiebeveiliging en privacy in hun jaarverantwoording op te nemen. Sommige besturen in het funderend onderwijs voldoen al langer aan die oproep van de minister van Onderwijs, Cultuur en Wetenschap (OCW). Maar nog niet alle besturen besteden in hun jaarverslag 2024 expliciet aandacht aan dit onderwerp. Het grootste deel van die jaarverslagen komt van besturen uit het funderend onderwijs. Als deze besturen en instellingen in de dagelijkse praktijk ook geen aandacht aan digitale weerbaarheid en veiligheid geven, zijn ze mogelijk minder bestand tegen digitale dreigingen en kwetsbaarder voor incidenten.
In het middelbaar beroepsonderwijs (mbo) en het ho (hoger onderwijs) bestaan al langere tijd bestuurlijke afspraken tussen de koepelorganisaties, het ministerie van OCW en ondersteunende partijen. Besturen in het mbo en ho benoemen dit thema al langer in hun jaarverslag.

Uit de brief van de minister van OCW aan de Tweede Kamer
"We verplichten schoolbesturen om vanaf schooljaar 2023/2024 in hun jaarverslag expliciet aandacht te besteden aan informatiebeveiliging en privacy (IBP). Dat zorgt ervoor dat besturen doordrongen raken van hun verantwoordelijkheid ten aanzien van digitale veiligheid en privacy." En: "Digitale veiligheid is niet alleen iets voor de ICT-verantwoordelijke, maar een verantwoordelijkheid van de hele school, van het bestuur tot en met de leraar in de klas. Daarom ondersteunen wij de professionalisering van het personeel binnen scholen, onder andere met bewustwordingscampagnes, een centraal scholingsaanbod en cybercrisisoefeningen."

Aanstaande Cyberbeveiligingswet vraagt meer inzet van hoger onderwijs

In de aanstaande Cyberbeveiligingswet krijgt de minister van OCW de bevoegdheid om instellingen in het hoger onderwijs aan te wijzen als belangrijke of essentiële entiteiten. In april 2025 maakte de minister al bekend dat hij dit ook echt wil doen. Vanaf de inwerkingtreding van deze wet hebben besturen in het ho een registratieplicht en een meldplicht bij significante incidenten. Ook moeten bestuursleden een training volgen om cyberveiligheidsaspecten mee te nemen in algemene besluitvorming. Ten slotte gaat 36 maanden na inwerkingtreding van de Cyberbeveiligingswet ook de zorgplicht uit de Cyberbeveiligingswet gelden voor de aangewezen hoger onderwijsinstellingen. Die maakt duidelijk welke maatregelen besturen moeten nemen om digitale risico's in hun instellingen duurzaam te beheersen.

Cyberbeveiligingswet

De Cyberbeveiligingswet is de Nederlandse implementatie van de Europese NIS2-richtlijn. NIS staat voor Network & Information Security. De NIS2-richtlijn is de aangescherpte versie van de NIS1-richtlijn. Iedere lidstaat vertaalt deze Europese richtlijn naar nationale wetgeving. De wet richt zich niet alleen op het onderwijs, maar op alle maatschappelijke sectoren. Voor het hoger onderwijs gaat de Cyberbeveiligingswet voorlopig enkel gelden voor de bekostigde instellingen. De minister van OCW is voornemens om de inspectie aan te wijzen als toezichthouder binnen het onderwijs. In andere maatschappelijke sectoren zijn straks andere toezichthouders actief. De inspectie wisselt wel kennis en kunde uit met deze toezichthouders.

Sommige besturen in het ho treffen al veel maatregelen op dit gebied. Andere besturen moeten straks aanzienlijk meer doen aan de digitale weerbaarheid en veiligheid van hun organisatie. Onderwijsinstellingen uit de andere sectoren vallen niet onder de Cyberbeveiligingswet, maar kunnen via hun leveranciers wel te maken krijgen met de gevolgen ervan. Leveranciers van de andere sectoren vallen in sommige gevallen namelijk ook onder de Cyberbeveiligingswet. De maatregelen die zij treffen, kunnen ook hun klanten raken.

Nuancering gebruikte data

De cijfers in dit rapport zijn gebaseerd op de verantwoording van onderwijsbesturen, zoals opgenomen in hun jaarverslagen. Deze jaarverslagen laten een grote diversiteit aan rapportages zien over digitale weerbaarheid en veiligheid. Ze geven inzicht in wat besturen zelf opnemen in hun jaarverslag, maar vormen dus niet per se een exacte weergave van de feitelijke situatie. Zo kunnen besturen besluiten een digitale dreiging, zoals een hack, vanwege lopend onderzoek of vertrouwelijkheid, niet op te nemen in het jaarverslag. Ook is het mogelijk dat een bestuur een datalek niet vermeldt in het jaarverslag omdat zij dat onnodig acht. Het is daarom belangrijk om de data met enige voorzichtigheid te interpreteren en deze te zien als indicatie van meld- en rapportagegedrag, niet als volledige opsomming van alle digitale incidenten en preventieve activiteiten in het onderwijs.

Analyse van aantallen

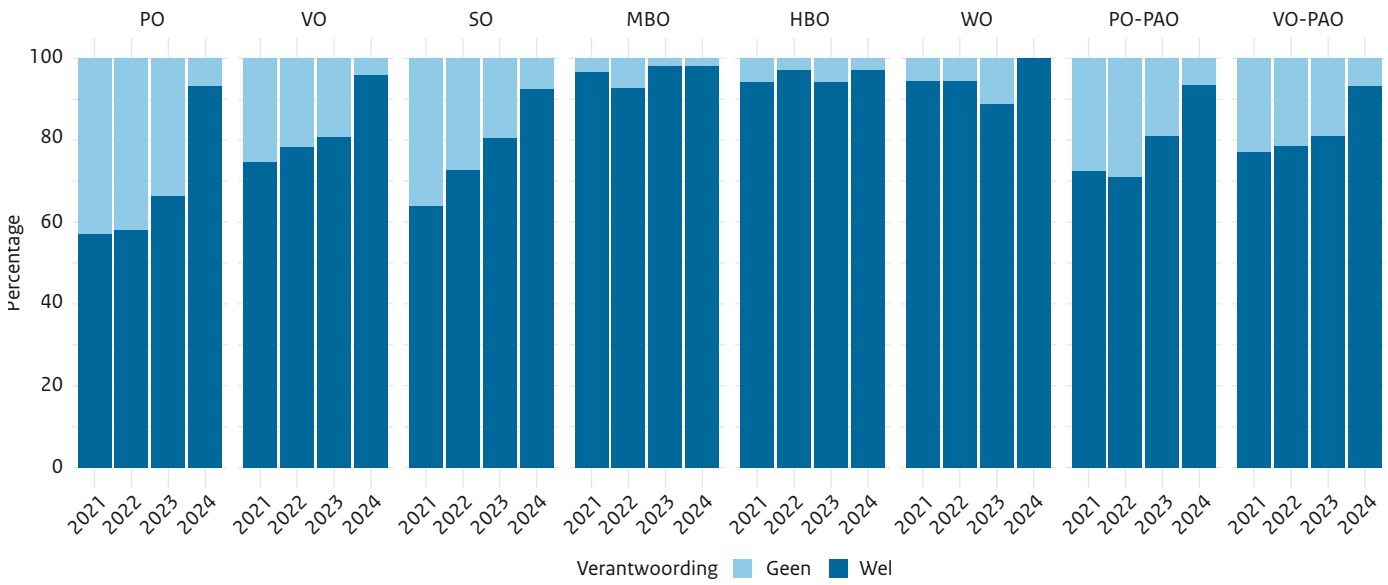
Het aandeel besturen dat aandacht besteedt aan digitale weerbaarheid en veiligheid is fors toegenomen

Vanaf 2024 zijn besturen in het funderend onderwijs verplicht in hun jaarverslag te rapporteren over informatiebeveiliging en privacy. Besturen van mbo- en ho-instellingen doen dit al meerdere jaren. In vergelijking met 2023 is het aantal besturen dat verantwoording aflegt over digitale weerbaarheid en veiligheid, sterk toegenomen.

Van alle besturen in het bekostigd onderwijs in Nederland besteedt 94% in het verslagjaar 2024 aandacht aan digitale weerbaarheid en veiligheid (zie figuur 1). Dit betekent dat zij minimaal één passage in hun jaarverslag hebben opgenomen waarin dit onderwerp aandacht krijgt. In 2023 was dit nog 74%. De grootste stijging doet zich voor in het po, waar het percentage steeg van 66% naar 93%. Ook in het vo, so en de samenwerkingsverbanden besteden inmiddels meer besturen aandacht aan digitale weerbaarheid en veiligheid. In het mbo, hbo en wo blijven de percentages redelijk stabiel. Het percentage besturen dat hierover rapporteert, verschilt in het verslagjaar 2024 nog maar weinig per sector, in tegenstelling tot voorgaande jaren. Dit laat zien dat verantwoording over dit onderwerp in alle onderwijssectoren meer gewicht heeft gekregen.

De cijfers laten óók zien dat er nog besturen zijn die in hun jaarverslag géén aandacht besteden aan digitale weerbaarheid en veiligheid. In 2024 ligt dat percentage op 6%. Dit kan overigens betekenen dat een bestuur wel maatregelen neemt, maar zich er niet over verantwoordt in het jaarverslag. Een mogelijke verklaring hiervoor is dat er te veel kwetsbaarheden zijn om over te rapporteren. Het kan ook betekenen dat een bestuur geen maatregelen neemt, omdat zij andere prioriteiten heeft. Voor de inspectie duidt het niet-rapporteren op een mogelijk risico. Het is belangrijk dat alle besturen de benodigde maatregelen treffen om de digitale weerbaarheid en veiligheid van de school te verhogen.

Figuur 1 – *Verantwoording over digitale weerbaarheid en veiligheid per sector per jaar*

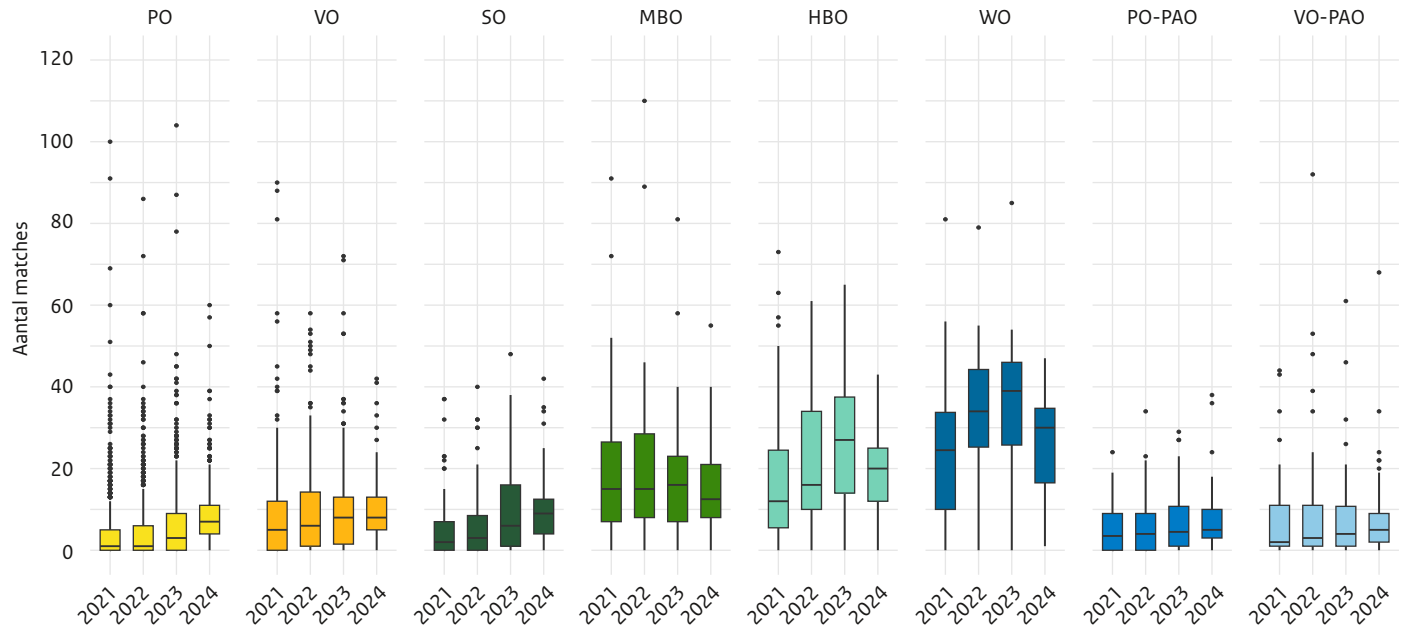


Minder variatie van het aantal passages per jaarverslag

Naast de aanwezigheid van verantwoording over digitale weerbaarheid en veiligheid is ook gekeken naar het aantal tekstpassages in een jaarverslag over dit onderwerp. Dit kan een indicatie zijn van urgentie van het thema. Ook kan het erop wijzen dat een bestuur meer diverse maatregelen treft.

De frequentie verschilt enorm tussen de sectoren (zie figuur 2). In het funderend onderwijs neemt deze sinds 2021 geleidelijk toe. Een mogelijke verklaring hiervoor is de groeiende maatschappelijke aandacht voor dit thema. In het mbo blijft de frequentie redelijk stabiel. In het hbo en wo stijgt deze tot 2023, maar daalt weer in 2024. De verantwoordingsfrequentie van besturen in het ho ligt gemiddeld nog steeds het hoogst. Over het algemeen nemen de uitschieters binnen de sectoren in 2024 af. Dat betekent dat verschillen in de frequentie binnen een sector kleiner worden. Verder liggen de frequenties tussen de sectoren in 2024 dichter bij elkaar. Dit duidt mogelijk op meer bewustzijn van het belang om over digitale weerbaarheid en veiligheid te rapporteren. De hoeveelheid opgenomen tekstpassages in het jaarverslag betekent overigens niet per se dat het beleid en de maatregelen doeltreffender zijn en ook niet per se dat de kwaliteit van de verantwoording beter is.

Figuur 2 – *Variatie van de verantwoordingsfrequentie per jaar per sector (aantal matches = frequentie van verantwoording)*



Drie bestuurskenmerken hangen samen met de frequentie

De inspectie voerde aanvullende analyses uit op de tekstpassages uit de jaarverslagen. We onderzochten de samenhang met diverse bestuurskenmerken om (een deel van) de verschillen te kunnen duiden. De 3 kenmerken die samenhangen met de verantwoordingsfrequentie zijn: de sector, de bestuursgrootte en het aantal leerlingen of studenten. De omvang van de totale begroting en de omvang van mogelijk bovenmatig eigen vermogen laten geen significante samenhang zien met de verantwoordingsfrequentie.

Besturen in het ho nemen de meeste passages over digitale weerbaarheid en veiligheid op in hun jaarverslag. In 2024 rapporteren wo-besturen hierover gemiddeld 26 keer en hbo-besturen gemiddeld 19 keer. Het mbo deed dit gemiddeld 16 keer. In het funderend onderwijs liggen de gemiddelden lager, maar dichter bij elkaar. So-besturen rapporteren 10 keer, vo-besturen 10 keer en po-besturen 8 keer.
Ook maakt de grootte van het bestuur uit voor de frequentie van verantwoording. We definiëren bestuursgrootte in het funderend onderwijs als het aantal scholen of afdelingen dat onder een bestuur valt. In het vervolgonderwijs gaat het om het aantal opleidingen dat onder een bestuur valt. Besturen met meer scholen, afdelingen of opleidingen rapporteren gemiddeld frequenter. Het effect van bestuursgrootte geldt los van de onderwijssector. Dat betekent dat een groot bestuur in het po gemiddeld meer over digitale weerbaarheid en veiligheid verantwoordt dan een klein bestuur in het hoger onderwijs. Het aantal leerlingen of studenten hangt samen met de verantwoordingsfrequentie. Besturen met meer leerlingen of studenten rapporteren gemiddeld iets frequenter over dit onderwerp, ongeacht de sector.
Tot slot, besturen met hogere baten rapporteren niet vaker dan besturen die lagere baten hebben. Hetzelfde geldt voor het eigen vermogen. Dit kan erop wijzen dat financiële middelen slechts een kleine rol spelen in het aantal tekstpassages over informatiebeveiliging en privacy in het jaarverslag.

Geen verandering in de inhoud van de verantwoording

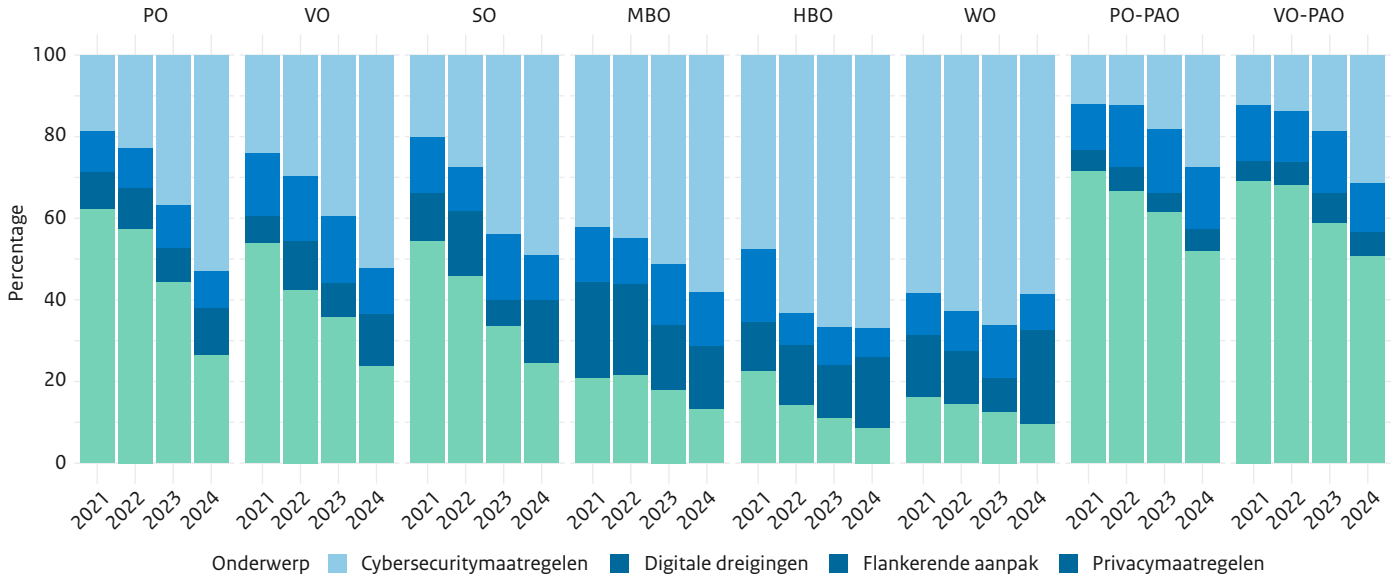
Verantwoording volgt op inhoudelijk handelen. Het is geen doel op zich, maar een manier om de voortgang zichtbaar te maken en te monitoren. Bij iedere tekstpassage kijkt de inspectie naar de manier waarop dit in het jaarverslag staat. Er zijn momenteel geen vormvereisten aan de details van verslaglegging anders dan de verplichting het onderwerp in het jaarverslag op te nemen.

Tussen 2021 en 2024 verandert er relatief weinig aan de wijze waarop dit thema in het jaarverslag inhoudelijk beschreven staat. In ongeveer 4 op de 5 passages (79%) ziet de inspectie elementen van de planning-en-controlcyclus terug. In 12% van de verantwoordingen leest de inspectie slechts een benoeming van een digitaal risico of een melding van een cyberincident. Hoe het bestuur hieraan vervolgens heeft gewerkt, blijkt niet uit de tekst. Het merendeel van de passages (64%) bevat concrete handelingen - zoals getroffen maatregelen of ingezet beleid – om digitale risico's te verkleinen of de herhaling van cyberincidenten te voorkomen. Een klein deel van de passages (6%) bevat een evaluatie. Daarin beschrijft het bestuur de effectiviteit van een maatregel, hoe zij dat monitort en vervolgens bijstuurt. In die passages ziet de inspectie alle elementen uit de planning-en-controlcyclus terugkomen. De overige 19% van de passages bevat onvoldoende informatie om ze over een van deze categorieën te verdelen.

Analyse van verantwoorde onderwerpen

We hebben de passages in de jaarverslagen van onderwijsinstellingen over digitale weerbaarheid en veiligheid onderverdeeld in vier thema's: cybersecuritymaatregelen, privacymaatregelen, flankerende aanpak en digitale dreigingen (zie figuur 3). Deze indeling toont over welke thema's besturen zich vooral verantwoorden. En hoe zij de digitale weerbaarheid en veiligheid van hun onderwijsinstelling aanpakken.

Figuur 3: *Verdeling van de vier thema's naar onderwijssector*



Cybersecurity: het dominante thema in 2024

In 2024 verantwoorden besturen zich het meest frequent over cybersecuritymaatregelen. Dit gaat om 50% van alle verantwoordingen in 2024. In 2021 was dit nog maar 28%. De relatieve stijging zien we ook terug in de absolute aantallen. In 2021 zijn er 2.585 passages over cybersecurity en in 2024 zijn er 6.251 passages. Besturen in het vervolgonderwijs rapporteren in eerdere jaren al het meest over dit thema. En dit blijft ook zo in 2024 (mbo 58%, hbo 67%, wo 59%). In het funderend onderwijs ligt vóór 2024 de nadruk in de jaarverslagen op privacymaatregelen. Dit accent verschoof de afgelopen jaren al, en in 2024 zijn cybersecuritymaatregelen ook in het funderend onderwijs het prominentste thema (po 53%, vo 52%, so 49%). De onderwijssectoren komen hiermee meer op dezelfde lijn. Een mogelijke verklaring voor deze verschuiving is de expliciete oproep door OCW tot verantwoording voor het funderend onderwijs.

Cybersecuritymaatregelen
Cybersecuritymaatregelen hebben betrekking op de technische bescherming van IT-systemen. Denk aan het invoeren van tweefactorauthenticatie (of multifactor-authenticatie), het uitvoeren van audits en het scheiden van gebruikersrollen binnen systemen. Deze maatregelen richten zich op het versterken van de digitale basisinfrastructuur. Binnen deze categorie analyseren we in hoeverre besturen zich wapenen tegen digitale dreigingen en in hoeverre zij aandacht besteden aan het beschermen van hun systemen.

Afname verantwoording over privacymaatregelen zet door

Besturen verantwoorden zich in hun jaarverslag van 2024 ten opzichte van eerdere jaren minder vaak over de privacymaatregelen. In 2021 gaat 46% van de verantwoordingen over privacymaatregelen en in 2024 is dit 26%. De relatieve daling zien we ook terug in de absolute aantallen. In 2021 zijn er 4.287 passages over privacymaatregelen en in 2024 zijn er 3.210 passages. Dit komt voor een groot deel door de stijging van passages over cybersecurity. De afname in verantwoording is het sterkst te zien bij instellingen in het funderend onderwijs. In het po gaat het aandeel over privacymaatregelen van 62% in 2021 naar 26% in 2024. En in zowel het vo als het so gaat dit aandeel van 54% in 2021 naar 24% in 2024. In het funderend onderwijs rapporteren besturen vaker over privacymaatregelen dan in het vervolgonderwijs (mbo 13%, hbo 9% en wo 9%). Bij de samenwerkingsverbanden po en vo gaan de meeste tekstpassages in 2024 wel over privacy: respectievelijk 52% in po-pao en 51% in vo-pao.

Privacymaatregelen
Privacymaatregelen komen voort uit de Algemene Verordening Gegevensbescherming (AVG) en gaan over de bescherming van persoonsgegevens. Voorbeelden zijn het aanstellen van een functionaris gegevensbescherming (FG), het opstellen van verwerkersovereenkomsten en het uitvoeren van Data Protection Impact Assessments (DPIA's).

Aandacht voor flankerende maatregelen toegenomen

In 2024 zien we in de jaarverslagen van onderwijsinstellingen toenemende aandacht voor gedragsmatige en organisatorische maatregelen die het digitale veiligheidsbeleid ondersteunen, de zogeheten flankerende maatregelen. Het aandeel van dergelijke passages schommelt sinds 2021. Respectievelijk ging 11% van de passages in 2021 over flankerende maatregelen, 12% in 2022, 10% in 2023 en 13% in 2024. Met name wo-instellingen vermelden deze maatregelen opvallend vaker in hun jaarverslag dan dat zij vorig jaar deden. In 2023 was dit nog het minst gerapporteerde thema bij wo-instellingen (8%) en in 2024 het op één na *meest* gerapporteerde thema (23%). Ook bij andere onderwijsinstellingen in het vervolgonderwijs vormen de flankerende maatregelen, na cybersecuritymaatregelen, het meest gerapporteerde thema (mbo 16%, hbo 17%). Onderwijsinstellingen in het funderend onderwijs leggen hier in hun jaarverslagen minder accent op, daar neemt dit thema de derde plaats in, na cybersecuritymaatregelen en privacymaatregelen (po 12%, vo 13%, so 16%). De toenemende aandacht voor flankerende maatregelen kan wijzen op een groter besef dat digitale weerbaarheid en veiligheid een onderwerp is dat de gehéle organisatie en álle medewerkers aangaat en niet slechts bij enkele medewerkers belegd kan zijn. Naast cybersecurity-maatregelen zijn flankerende maatregelen daarom belangrijk bij het detecteren van digitale dreigingen en voor het voorkómen van incidenten. En ze dragen bij aan het bewustzijn dat medewerkers onderdeel zijn van het gehele beveiligingssysteem. Wie als medewerker toegangsrechten krijgt, moet ook weten dat je daar zorgvuldig mee moet omgaan. Zeker als die rechten toegang geven tot gevoelige persoonsgegevens, onderwijs- en/of onderzoeksdata.

Flankerende maatregelen
Flankerende maatregelen zijn gedragsmatige en organisatorische maatregelen die het digitale veiligheidsbeleid ondersteunen. Denk aan het beleggen van IBP-verantwoordelijkheden binnen de organisatie, het organiseren van bewustwordingscampagnes of het trainen van medewerkers in veilig digitaal handelen.

Beperkte aandacht voor digitale dreigingen neemt nog iets verder af

Besturen besteden in de jaarverslagen in 2024 relatief het minst aandacht aan concrete risico's of incidenten. Met 1.407 verantwoordingen betreft dit 11% van alle passages. In bijna alle sectoren (behalve het mbo en de samenwerkingsverbanden passend onderwijs) is dit het geval. Dit valt op, omdat er in het funderend onderwijs wel degelijk sprake is van meer cyberaanvallen waarmee onderwijsinstellingen te maken krijgen (zie Dreigingsbeeld Funderend Onderwijs Kennisnet). In het hbo gaat slechts 7% van de verantwoordingen over digitale dreigingen en in het wo is dat 9%. Onderwijsinstellingen in het funderend onderwijs laten een redelijk vergelijkbaar beeld zien (po 9%, vo 11%, so 11%). Het mbo besteedt met 13% nog het meest aandacht aan digitale dreigingen.

Digitale dreigingen
De categorie digitale dreigingen heeft betrekking op concrete risico's of incidenten, zoals datalekken, hacks, phishing of DDoS-aanvallen. Deze categorie biedt inzicht in de kwetsbaar-heden waarmee besturen kunnen worden geconfronteerd en de manier waarop zij daarover rapporteren.

Weinig aandacht voor digitale incidenten is een gemiste kans

Van alle tekstpassages in de jaarverslagen over 2024 beschrijft 4% een digitaal incident. Van alle besturen rapporteert 20% over één of meerdere digitale incidenten die bij de onderwijsinstelling zelf plaatsvinden. Dat betekent dat 1 op de 5 besturen weliswaar aandacht besteedt aan digitale incidenten, maar dat de aandacht voor andere onderwerpen bij alle besturen heel veel groter is. Deze cijfers willen overigens niet per se zeggen dat alle digitale incidenten in het jaarverslag staan.

We weten daarnaast dat menselijke fouten of onzorgvuldig gegevensgebruik de grootste oorzaken zijn van digitale incidenten (Monitor Digitale Weerbaarheid en Veiligheid 2024 - Inspectie). Toch laten besturen in de meeste gevallen de bron en de oorzaak van een incident achterwege. Ook rapporteren zij meestal niet over de impact van een incident op de organisatie en het onderwijs. Dit is een gemiste kans voor het gehele onderwijsstelsel. Want besturen die transparant rapporteren over cyberincidenten, de afwikkeling daarvan en aangepaste maatregelen of beleid, geven daarmee ook inzicht in de leercurve van hun organisatie. Het is daarbij uiteraard niet de bedoeling een specificatie van actuele risico's en kwetsbaarheden in het jaarverslag te vermelden. Een transparante verantwoording over afgehandelde incidenten helpt andere besturen om daarvan te leren voor hun eigen digitale weerbaarheid en veiligheid.

De urgentie van digitale weerbaarheid en veiligheid

Blijf aandacht besteden aan digitale weerbaarheid en veiligheid

Aanhoudende digitale dreigingen

Het realiseren van digitale weerbaarheid en veiligheid is een noodzakelijk onderdeel van goed bestuur binnen het onderwijs. Onderwijsinstellingen maken in toenemende mate gebruik van digitale middelen. Daarmee groeit hun afhankelijkheid van een veilige en betrouwbare digitale infrastructuur. Dit brengt niet alleen mogelijkheden en kansen, maar ook risico's met zich mee. Het maakt onderwijsinstellingen kwetsbaar voor bijvoorbeeld hacks, phishing, malware, DDoS-aanvallen en datalekken. Cybercriminelen zoeken elke keer weer nieuwe manieren om een onderwijsorganisatie binnen te dringen. Volgens SURF maakt de opkomst van artificiële intelligentie (AI) het nog gemakkelijker om aanvallen uit te voeren (Cyberdreigingsbeeld onderwijs en onderzoek 2025). De ernst van de dreigingen moet dan ook niet onderschat worden. In het tweede kwartaal van 2024 stond de Amerikaanse onderwijssector op de derde plaats van meest aangevallen sectoren (Microsoft). En de VO Raad schrijft in 2025 dat het geen kwestie is van 'of', maar van 'wanneer' een cyberincident zich in een onderwijsinstelling aandient. De omvang van digitale dreigingen en de daaruit voortvloeiende schadelijke gevolgen groeit. En daarmee ook de noodzaak om maatregelen te treffen.

Grote gevolgen voor het onderwijs

Digitale incidenten kunnen grote gevolgen hebben. Cybercriminelen kunnen toegang tot systemen blokkeren en IT-afdelingen moeten systemen soms uit voorzorg uitzetten. Dit bedreigt de continuïteit. Denk aan het uitvallen van lessen en het niet kunnen afnemen van toetsen. Ook kunnen cybercriminelen persoonsgegevens bewerken of zelfs stelen, waardoor de school niet meer de juiste gegevens heeft om het meest passende onderwijs te kunnen aanbieden. Ook is de privacy dan in het geding.

De inspectie ziet dat een omvangrijk cyberincident vaak een lange nasleep kent en altijd grote gevolgen voor de organisatie heeft.

Digitale verstoringen komen naast zulke externe dreigingen ook voort uit interne dreigingen (Monitor Digitale Weerbaarheid en Veiligheid 2024 - Inspectie). Hierbij valt te denken aan datalekken door menselijke fouten, onzorgvuldig gebruik van persoonsgegevens of incidenten binnen de eigen beveiliging. Hoewel het accent in de jaarverslagen niet meer bij de privacymaatregelen ligt, blijven intern datalekken de meest voorkomende incidenten. En ook interne dreigingen kunnen de onderwijsprocessen raken.

Ketenafhankelijkheid

Naast de incidenten die een onderwijsinstelling direct kunnen treffen, kunnen incidenten bij partners van deze instellingen óók een bedreiging vormen. Dit komt door hun afhankelijkheid binnen de keten. Uit de datalekkenrapportage 2024 van de AP blijkt dat de sector Onderwijs dat jaar een van de meest getroffen sectoren was op het gebied van cyberaanvallen. Een groot deel van deze meldingen is terug te leiden tot de ransomware-aanval op schoolboekenleverancier Iddink in 2024. Deze dynamiek illustreert de mate van ketenafhankelijkheid op digitaal gebied. Bij het uitbesteden van taken aan toeleveranciers blijft de onderwijsinstelling zelf verantwoordelijk voor gegevensbescherming. Besturen moeten daarom vastleggen hoe hun leverancier met de data moet omgaan en zorgen dat ze hier zicht op houden.

Wettelijke verplichting funderend onderwijs

Onderwijsinstellingen in het funderend onderwijs moeten wettelijk hun digitale weerbaarheid en veiligheid structureel borgen binnen hun bestuurlijke kwaliteitszorg. Bestuurders moeten dus risico's herkennen, maatregelen treffen en zorgen voor voldoende deskundigheid binnen de onderwijsinstelling. Digitale weerbaarheid en veiligheid is daarmee niet alleen een technische kwestie, maar óók een organisatorische en ethische verantwoordelijkheid. Goed bestuur betekent dan ook dat instellingen hun digitale risico's periodiek evalueren en op basis daarvan de noodzakelijke maatregelen treffen. Een goed hulpmiddel voor besturen bij het borgen van de digitale weerbaarheid en veiligheid is het Normenkader IBP. Het helpt daarnaast als onderwijsinstellingen oefenen met crisissituaties, net als een ontruimingsoefening bij een brand. SURF organiseert de cybercrisisoefening NOZON voor instellingen in het mbo en ho. School-CERT doet dit ook voor het funderend onderwijs. Een ander voorbeeld is het werken met ethisch hackers om kwetsbaarheden op te sporen. Ook samenwerking binnen onderwijsnetwerken en met deskundige partijen is belangrijk. Zorgvuldige transparantie komt het hele veld ten goede: hoe meer besturen laten zien hoe zij zelf omgaan met digitale dreigingen en veiligheid, hoe meer andere besturen hiervan kunnen leren. Belangrijk, want digitale weerbaarheid en veiligheid is een randvoorwaarde voor betrouwbaar, toekomstbestendig en veilig onderwijs.

Inwerkingtreding van de Cyberbeveiligingswet

Met de inwerkingtreding van de Cyberbeveiligingswet promoveert digitale veiligheid in het hoger onderwijs van een IT-onderwerp naar een strategische prioriteit. De aanvullende verplichtingen dwingen de besturen van de instellingen immers om digitale weerbaarheid structureel te verankeren in hun bedrijfsvoering. Dit is geen eenmalige exercitie, maar een voortdurend proces van risicomanagement en cultuurverandering. Het speelt zich af in een landschap waarin dreigingen sneller muteren dan de gemiddelde software-update. Een proactieve houding vergroot de kans om continuïteit van onderwijs en onderzoek te waarborgen. Dit vraagt

om gerichte keuzes van het bestuur op basis van een specifieke risico-inschatting. Door inventieve oplossingen kan het onderwijs ook morgen, volgende maand en volgend jaar doorgaan. Ook andere onderwijssectoren die nu (nog) niet onder de Cyberbeveiligingswet vallen, kunnen er op termijn wel degelijk hun voordeel mee doen.

Transparantie dient het héle onderwijsveld

De verantwoording van maatregelen op het gebied van digitale weerbaarheid en veiligheid in jaarverslagen dient de systeemvolwassenheid van het gehele onderwijsveld. Aan de ene kant biedt het meer inzicht in de digitale risico's en de veelheid aan dreigingen waarmee het onderwijs te maken heeft. Aan de andere kant kan adequate verslaglegging van bijzonder effectieve maatregelen een inspiratiebron zijn voor andere onderwijsinstellingen. Het is tegelijk onverstandig om kwetsbaarheden in het jaarverslag te vermelden. Daarom besteden we in het laatste deel van deze monitor aandacht aan bestaande hulpmiddelen om dit thema zorgvuldig in het jaarverslag op te nemen.

Handreikingen voor het onderwijsveld over verantwoording in jaarverslagen

Er bestaan diverse handreikingen voor het onderwijsveld over het afleggen van verantwoording over digitale weerbaarheid en veiligheid in jaarverslagen. De inspectie onderschrijft deze handreikingen en licht ze hier graag toe.

- De VO-raad en PO-Raad adviseren te benoemen waar in het verleden risico's waren en hoe deze (beleidsmatig) zijn aangepakt, vernieuwd of verholpen. Zij ontraden echter nadrukkelijk om een specificatie van actuele risico's en kwetsbaarheden in het jaarverslag te vermelden. Op de websites van de raden staat een algemene handreiking voor het schrijven van het bestuursverslag, waarin ook suggesties voor het benoemen van de digitale weerbaarheid en veiligheid zijn opgenomen. Zie de handreikingen van de VO-raad en de PO-Raad. Deze handreikingen sluiten aan bij de brief van 15 december 2025, die de besturen van OCW hebben ontvangen.
- Daarnaast biedt SURF voor het mbo en ho een uitgebreide handreiking voor verantwoording in het jaarverslag, toegespitst op cyberbeveiliging. Ook SURF benadrukt goed rekening te houden met het vertrouwelijke karakter van de informatie. Op hun site staat een handreiking met vragen die hiervoor als leidraad kunnen dienen.
- Een derde set aanbevelingen staat in het inspectierapport "Binnen zonder kloppen". Dit rapport is opgesteld na de cyberaanval op Maastricht University in 2019. Hoewel het zich in de eerste plaats richt op het ho, kunnen de aanbevelingen dienen als bron van inspiratie voor het hele onderwijsveld.

In alle onderwijssectoren kunnen deze handleidingen helpen om digitale dreigingen beter in kaart te brengen en te beheersen. De inspectie ziet ruimte om met elkaar optimale verslaglegging van maatregelen op het gebied van digitale weerbaarheid en veiligheid te ontwikkelen. De basis hiervoor is kennisdeling, samenwerking en dialoog.

Samen voorbereiden op digitale dreigingen

Leren van elkaar

We weten vaak niet wat we niet weten. Dit geldt in algemene zin voor veel zaken, maar voor digitale weerbaarheid en veiligheid in het bijzonder. Er is immers veel ongewis op het gebied van cybercriminaliteit en het dreigingsbeeld verplaatst zich voortdurend en in onvoorspelbare richtingen. Wat wel duidelijk is, is dat we als scholen en instellingen allemaal in dezelfde situatie zitten. Digitale vraagstukken raken het hele onderwijsveld, net als andere maatschappelijke sectoren. Ook internationaal speelt de vraag hoe we digitaal weerbaar en veilig worden en blijven. Leren over de aard van digitale risico's is essentieel. Samen weten we meer. De inspectie ziet daarom de rapportages in jaarverslagen als potentiële bron van informatie voor de rest van het onderwijsveld. Denk hierbij aan transparantie over de ervaren digitale dreigingen bij de instelling en uitwerking van de geboden oplossingen. Ook vinden regelmatig congressen en workshops over dit onderwerp plaats. De dialoog biedt inspiratie voor aanpassingen en oplossingen. Het rapporteren en met elkaar praten over het thema leidt tot betere bewustwording en voorbereiding. Door adequate kennisdeling van een cyberincident kunnen onderwijsinstellingen van elkaar leren. De inspectie blijft digitale weerbaarheid en veiligheid en de verantwoordingen in de jaarverslagen hierover monitoren.

Basisprincipes van digitale weerbaarheid van het Nationaal Cyber Security Centrum (NCSC):

"Veel digitale incidenten vinden hun oorzaak in het niet op orde hebben van basisbeveiligingsmaatregelen. Dat is jammer, want vaak maak je met relatief eenvoudige stappen je organisatie een stuk digitaal weerbaarder." Om te komen tot een gezonde en degelijke cyberbeveiligingsstrategie publiceerde het NCSC 5 basisprincipes van digitale weerbaarheid. Voor scholen in het funderend onderwijs is Kennisnet – naast de sectorraden – een goede informatiebron voor praktische hulp bij het vormgeven van digitale weerbaarheid en veiligheid. Kijk op hun website. Kennisnet heeft 11 basismaatregelen beschreven, mede geïnspireerd op de basisprincipes van het NCSC. Het vervolgonderwijs kan terecht bij SURF en MBO Digitaal voor praktische handreikingen en aanvullende informatie over cyberveiligheid.

Colofon

Foto voorpagina: Bert Kasteel

Inspectie van het Onderwijs
Postbus 2730 | 3500 GS Utrecht

Een exemplaar van deze publicatie is te downloaden van de website van de Inspectie van het Onderwijs
www.onderwijsinspectie.nl