Inspectie van het Onderwijs
Ministerie van Onderwijs, Cultuur en Wetenschap

Digitale weerbaarheid en veiligheid in jaarverslagen
Monitor digitale weerbaarheid en veiligheid

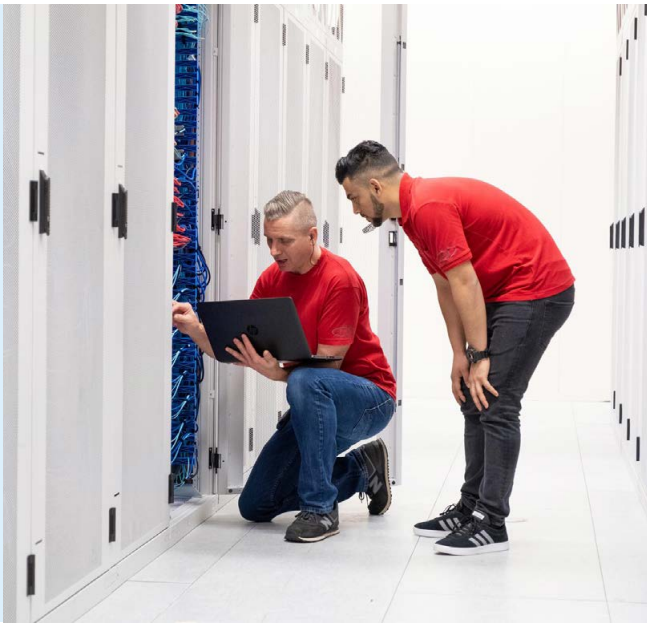
September 2025

Hoeveel besturen besteden in hun jaarverslag aandacht aan digitale weerbaarheid en veiligheid? In juli 2022 riep de minister hen op om hun aanpak van digitale veiligheid in het jaarverslag te verantwoorden. In deze monitor leest u hoeveel besturen hier in hun jaarverslag over 2021, 2022 en 2023 uit zichzelf al gehoor aan gaven en wat hen kenmerkt.

Voorwoord

Dagelijks gaan miljoenen leerlingen, studenten en docenten naar hun school of opleiding. Voor al die mensen is het belangrijk dat het onderwijs dag in dag uit doorgaat. Veel besturen zorgen al dat dat kan door het gesprek te voeren over de digitale weerbaarheid van hun organisatie. Want: wat heb je nodig om onderwijs door te laten gaan na een digitaal incident? Beschik je over de correcte gegevens van leerlingen en studenten? Wat doe je om te voorkomen dat gegevens in verkeerde handen komen? Pak die bal op en blijf niet achter.

Alida Oppers
inspecteur-generaal van het Onderwijs



Samenvatting

- **Besturen verantwoorden zich vaker** - in 2021 rapporteerde 65% van de besturen over digitale weerbaarheid en veiligheid in hun jaarverslag. In 2023 was dit 74%.
- **Grote verschillen tussen sectoren** - het middelbaar beroepsonderwijs en hoger onderwijs lopen voorop in verantwoording over digitale weerbaarheid en veiligheid; het primair en voortgezet onderwijs blijven achter.
- **Grotere besturen rapporteren vaker** - grotere besturen verantwoorden zich structureel vaker dan kleinere instellingen. Dit patroon is zichtbaar in alle sectoren.
- **Onderwerpen verschillen per sector** - besturen in het funderend onderwijs richten zich vooral op privacy. Het middelbaar beroepsonderwijs en hoger onderwijs gaan vaker in op cybersecurity.
- **Digitale incidenten weinig gemeld** - jaarverslagen bevatten weinig meldingen van digitale dreigingen (zoals een datalek, hack, phishing of DDoS-aanval). De meeste vermelde incidenten blijken intern veroorzaakt.
- **Beperkt aandacht voor gedragsmaatregelen om risico's te verminderen** - besturen rapporteren relatief weinig over bijvoorbeeld bewustwordings-activiteiten of trainingen voor personeel.

Aanleiding

Informatietechnologie (IT) is sterk verweven met het onderwijs. Zo biedt IT docenten, studenten en leerlingen veel mogelijkheden om informatie te zoeken en contacten te leggen over de hele wereld. De verwevenheid vraagt van besturen om scholen en opleidingen weerbaar te maken tegen digitale dreigingen. Besturen moeten daarom het beleid rondom digitale weerbaarheid en veiligheid op orde brengen en houden. Onderwijs moet door kunnen gaan, ook als de IT tijdelijk niet werkt. Daarnaast is veilige opslag van de juiste onderwijsdata van belang om zicht te houden op leerlingen en studenten en om diploma's uit te kunnen reiken. Een digitaal veilige leeromgeving betekent ook zorgdragen voor persoonsgegevens van leerlingen, studenten en medewerkers. Deze dreigingen zijn niet fictief. Scholen en instellingen van basisonderwijs tot aan universiteit hebben hier al mee te maken gehad. Ook incidenten in de keten, zoals een hack bij een leverancier van schoolmiddelen, raken het onderwijs.

Besturen in het funderend onderwijs waren tot en met het verslagjaar 2023 nog niet verplicht om over digitale weerbaarheid en veiligheid te rapporteren. Toch hebben de ministers van Onderwijs, Cultuur en Wetenschap (OCW) in verschillende kamerbrieven sinds 2022 opgeroepen om in de jaarverslagen aandacht te besteden aan dit thema.[1] Vanaf verslagjaar 2024 is de vrijblijvendheid eraf: informatiebeveiliging en privacy vormen één van de maatschappelijke thema's waarover besturen in het funderend onderwijs zich in hun jaarverslag moeten verantwoorden. De koepels van mbo en ho hebben over dit thema afspraken gemaakt met OCW en ondersteunende partijen. Daarom verwacht de inspectie dat besturen hierover rapporteren in het jaarverslag. Dit onderzoek brengt in kaart in welke mate besturen in hun jaarverslagen over 2021, 2022 en 2023 aandacht besteedden aan digitale weerbaarheid en veiligheid.

Om besturen in het funderend onderwijs te ondersteunen, werken het ministerie van OCW, Kennisnet, Sivon, de PO-Raad en de VO-raad samen in het programma Digitaal Veilig Onderwijs. In 2024 is het School-CERT gestart. CERT staat voor Computer Emergency Response Team. Dit team bestaat uit gespecialiseerde IT-professionals en kan besturen adviseren in geval van een cybersecurity-incident. Voor het mbo en ho vervult SURF-CERT deze functie al langere tijd. Daarnaast ontwikkelde het programma het Normenkader Informatiebeveiliging en Privacy (IBP) voor het funderend onderwijs. Voor het mbo en ho heeft SURF toetsingskaders voor informatiebeveiliging en voor privacy. De MBO-Raad, Vereniging Hogescholen en Universiteiten van Nederland maakten met OCW afspraken over het volwassenheidsniveau waaraan mbo en ho instellingen moeten voldoen. MBO-digitaal heeft het programma cyberveiligheid dat mbo-instellingen ondersteunt bij het verhogen van hun digitale weerbaarheid.

Nuancering gebruikte data

De cijfers in dit rapport zijn gebaseerd op de verantwoording van onderwijsbesturen, zoals opgenomen in hun jaarverslagen. Ze geven daarmee inzicht in wat besturen zelf opnemen in hun jaarverslag, maar vormen niet per se een exacte weergave van de feitelijke situatie. Zo kunnen besturen een digitale dreiging, zoals een hack, vanwege lopend onderzoek of vertrouwelijkheid, niet altijd opnemen in het jaarverslag. Ook is het mogelijk dat een bestuur een datalek niet opneemt in het jaarverslag omdat zij dat onnodig acht. Het is daarom belangrijk om de data met de nodige voorzichtigheid te interpreteren en deze te zien als indicatie van meld- en rapportagegedrag, niet als volledig beeld van alle digitale incidenten en preventieve activiteiten in het onderwijs.

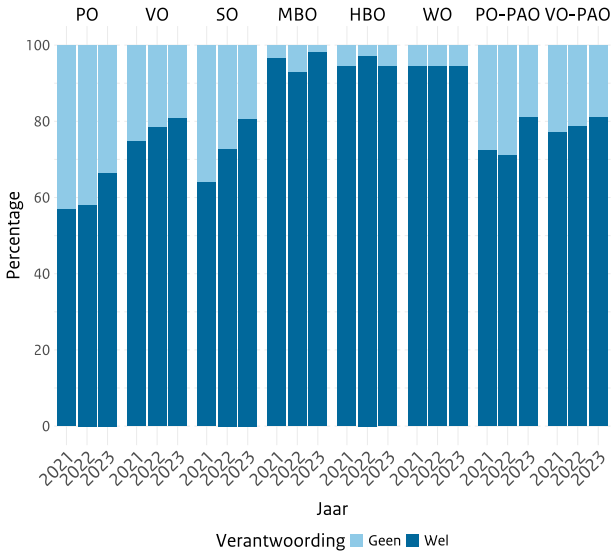
1 Kamerbrief over verhogen digitale veiligheid onderwijs en onderzoek | Kamerstuk | Rijksoverheid.nl 14-07-2022; Kamerbrief over digitalisering in funderend onderwijs | Kamerstuk | Rijksoverheid.nl 6-07-2023; Digitalisering en leermiddelen in het funderend onderwijs | Kamerstuk | Rijksoverheid.nl 22-11-2024; Kamerbrief over voortgang cyberweerbaarheid in het vervolgonderwijs | Kamerstuk | Rijksoverheid.nl 24-04-2025

Analyse van aantallen (kwantitatieve analyse)

Geleidelijke toename verantwoordingen

De verantwoording over digitale weerbaarheid en veiligheid is de afgelopen jaren in alle sectoren toegenomen en met name in het funderend onderwijs. Het aantal besturen dat zich verantwoordt neemt toe. Het aandeel verantwoordende besturen in het primair onderwijs (po) ligt met 66% nog relatief laag. Het ziet ernaar uit dat het po iets later startte met structureel rapporteren over digitale veiligheid. Besturen in het middelbaar beroepsonderwijs (mbo) en hoger onderwijs (ho) verantwoorden zich vaker en uitgebreider over informatiebeveiliging en privacy (ibp).

In het jaarverslag 2023 besteedde bijna driekwart van de besturen op een of andere wijze aandacht aan het onderwerp digitale weerbaarheid en veiligheid (zie figuur 1). In totaal bevatten 972 jaarverslagen één of meer verantwoordingen over digitale weerbaarheid en veiligheid. Er is sprake van een geleidelijke toename van de verantwoording in de jaren 2021 (65%), 2022 (67%) en 2023 (74%).



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

Het percentage besturen dat zich verantwoordt over digitale weerbaarheid en veiligheid verschilt nog per sector. In het mbo, hbo en wetenschappelijk onderwijs (wo) bevatten bijna alle jaarverslagen over 2023 verantwoordingen over digitale weerbaarheid en veiligheid (respectievelijk 98%, 94% en 94%). In het funderend onderwijs varieert dit tussen 66% (po), 81% (voortgezet onderwijs (vo)) en 81% (speciaal onderwijs (so)). Van alle samenwerkingsverbanden verantwoordt 81% zich in 2023 over digitale weerbaarheid en veiligheid. Dit houdt in dat 261 besturen in het po zich niet verantwoorden in hun jaarverslag 2023 over de wijze waarop ze invulling gaven aan hun digitale weerbaarheid.
In alle sectoren is groei zichtbaar in de hoeveelheid besturen met verantwoordingen over digitale weerbaarheid en veiligheid. Tussen 2021 en 2023 maakte het so de grootste groei door in het percentage instellingen dat verantwoording aflegt: van 64% naar 81%. Het po kende een toename van 57% naar 66%. Het mbo laat een lichte groei zien van 97% naar 98%.

Hieruit blijkt dat een zeer hoog aantal van de besturen in deze sector zich verantwoordt over dit onderwerp. De minste groei is zichtbaar in het hbo en wo. Daar bleef het percentage voor beide gelijk, op 94%.

De cijfers laten zien dat verantwoording over digitale weerbaarheid en veiligheid in alle sectoren toeneemt, met name in het funderend onderwijs. Deze groei hangt mogelijk samen met het in 2023 gepubliceerde Normenkader Informatiebeveiliging en Privacy voor het onderwijs en de verwachting dat alle po- en vo-scholen eind 2027 dit kader moeten toepassen. Tegelijkertijd zijn er nog steeds grote verschillen tussen sectoren en blijft het funderend onderwijs achter op het hoger onderwijs in de mate van verantwoording. Een mogelijke verklaring hiervoor is dat er in het mbo, hbo en wo al langer bestuurlijke afspraken bestaan over ibp dan in het funderend onderwijs.

Meer verantwoordingen in het vervolgonderwijs

De mate waarin onderwijsbesturen aandacht besteden aan digitale weerbaarheid en veiligheid verschilt sterk per sector. Besturen in het hoger onderwijs rapporteren gemiddeld vaker en uitgebreider dan in het funderend onderwijs. Dit komt vermoedelijk door verschillen in capaciteit en het strategisch belang van digitale veiligheid.

Het gemiddeld aantal verantwoordingen over digitale weerbaarheid en veiligheid varieert per sector.
Gemiddeld rapporteren po-besturen hierover 6 keer in hun jaarverslag 2023. Wo-besturen verantwoorden datzelfde jaar gemiddeld 35 keer. De spreiding ten opzichte van het gemiddelde is groter in de sectoren waar het gemiddeld aantal verantwoordingen hoger ligt. In de sectoren mbo en ho varieert het aantal verantwoordingen tussen besturen het sterkst. De meerderheid van de besturen in deze sectoren besteedt tussen 3 en 57 keer aandacht aan digitale weerbaarheid en veiligheid in hun jaarverslag in 2023, terwijl dit bereik in het funderend onderwijs tussen 0 en 22 ligt.

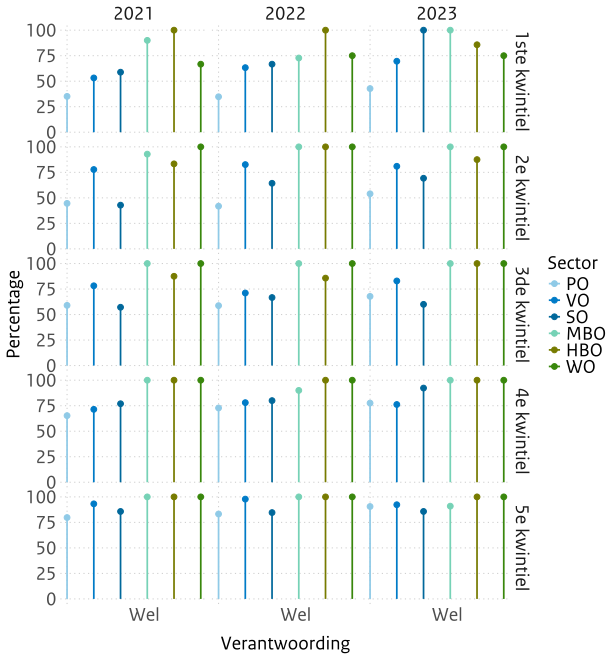
De verschillen suggereren dat besturen in het ho uitvoeriger rapporteren over digitale weerbaarheid en veiligheid dan besturen in het funderend onderwijs. Dit kan samenhangen met grotere beleidsmatige en technische capaciteit, in combinatie met het grotere belang van digitale veiligheid binnen deze instellingen. Bijvoorbeeld vanwege het beschermen van gevoelige kennis en data, zoals in digitale leeromgevingen en onderzoekspraktijken.

Grotere besturen verantwoorden vaker

Bestuursomvang hangt sterk samen met de mate van verantwoording over digitale weerbaarheid en veiligheid. Grotere besturen verantwoorden structureel vaker dan kleinere instellingen. Dit patroon is zichtbaar in alle sectoren.

De mate van verantwoording over digitale weerbaarheid en veiligheid verschilt per omvang van het bestuur, gemeten in aantal leerlingen of studenten (zie figuur 2). De omvang is gebaseerd op de relatieve omvang binnen de sector (dus niet op absolute aantallen). Besturen met de meeste leerlingen of studenten rapporteren in 2023 het vaakst over digitale weerbaarheid en veiligheid. In het po doet 91% van de besturen

dat, in het vo 92% en in het so 86%. Bij de groep besturen met de minste leerlingen ligt dit aandeel aanzienlijk lager in het po (43%) en vo (70%), terwijl in het so juist alle besturen (100%) verantwoording afleggen.



Figuur 2 - *Verantwoording naar aantal leerlingen en studenten*

Binnen het mbo ligt de verantwoording boven de 90% in alle groepen besturen van verschillende omvang. Alle kleine tot middelgrote besturen in het mbo rapporteerden in 2023 over digitale weerbaarheid en veiligheid. Opvallend is dat juist in het segment met de grootste besturen 1 van de 11 besturen geen verantwoording aflegde. Dit bestuur vormt bovendien het enige mbo-bestuur in 2021, 2022 of 2023 zonder verantwoording over digitale weerbaarheid en veiligheid in het jaarverslag. Dit laat zien dat de omvang van een bestuur niet uitsluitend de mate van verantwoording bepaalt.

In 2023 verantwoordde 94% van de ho-besturen en 94% van de wo-besturen zich over digitale weerbaarheid en veiligheid. 3 besturen legden geen verantwoording af over dit thema. Dit betrof 2 van de 35 besturen in het hbo en 1 van de 18 besturen in het wo. Opvallend is dat het in alle 3 de gevallen gaat om instellingen met een relatief klein studentenbestand: ze vallen binnen de omvangsklasse van 1 tot 7.499 studenten. Net als in andere sectoren zijn het met name de kleinere instellingen die geen verantwoording opnemen in hun jaarverslag. In beide sectoren ligt de verantwoording bij instellingen met een groter studentenaantal structureel hoger.

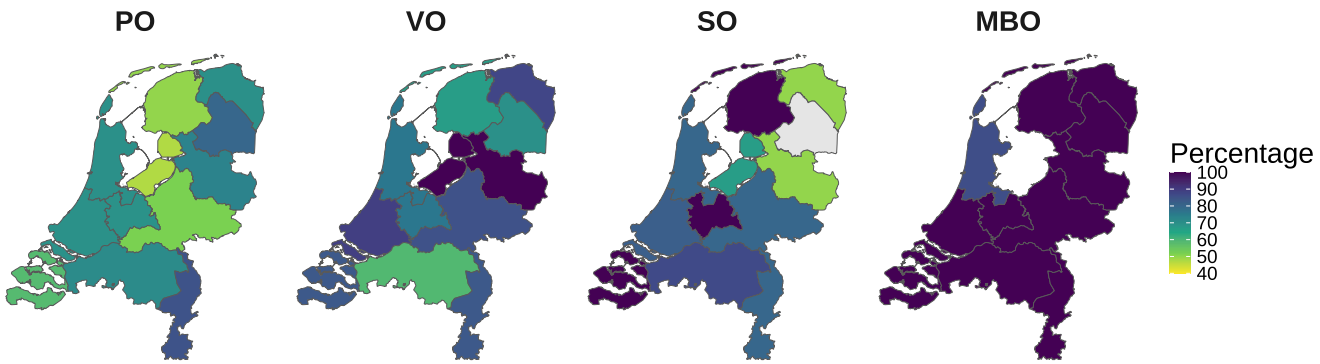
Groei in percentage verantwoordingen vooral bij kleinste (po-)besturen

In 2023 is er voor po, vo en so in bijna alle groepen besturen van verschillende omvang sprake van een toename in verantwoording ten opzichte van 2021. Figuur 2 laat zien dat de groei het sterkst zichtbaar is bij de kleinste po-besturen. In deze groep nam het aandeel verantwoordende besturen toe van 35% naar 43%. Ook binnen het vo is over het algemeen sprake van groei, met een gemiddelde stijging van 6%. Alleen in de groep met de grootste besturen in het vo is sprake van een lichte daling (van 93% naar 92%), al blijft het percentage daarmee nog steeds uitzonderlijk hoog. Dit benadrukt dat ook besturen waarvoor verantwoording over digitale weerbaarheid en veiligheid nog niet verplicht was, hier in brede zin toch al werk van maken. Binnen het so groeide het aandeel verantwoordende besturen in de groep met de op één na kleinste besturen van 43% naar 70%. Daarmee is zichtbaar dat de aandacht voor digitale weerbaarheid en veiligheid toeneemt, ongeacht de schaal waarop een bestuur opereert.

Geen regionaal patroon zichtbaar

Hoewel de verantwoording over digitale weerbaarheid en veiligheid landelijk toeneemt, blijven sommige regio's achter, vooral in het po. Maar er bestaat geen consistent patroon tussen regio en rapportagegedrag.

In figuur 3 is te zien dat over de hele linie een stijgend aandeel besturen verantwoording aflegt, maar met name in het po blijven sommige regio's achter. Terwijl regio's als Drenthe (van 60% naar 80%), Limburg (van 69% naar 85%) en Overijssel (van 60% naar 73%) duidelijke groei laten zien, valt op dat het aandeel verantwoordingen in Flevoland daalt van 53% naar 47%, en in Zeeland zelfs afneemt van 68% naar 59%. Er zijn geen duidelijke patronen zichtbaar tussen regio en verantwoordingen over digitale weerbaarheid en veiligheid. Ook valt op basis van de data nog geen uitspraak te doen over het mogelijke effect van zichtbare incidenten in een regio op de bewustwording of rapportagebereidheid van omliggende besturen.

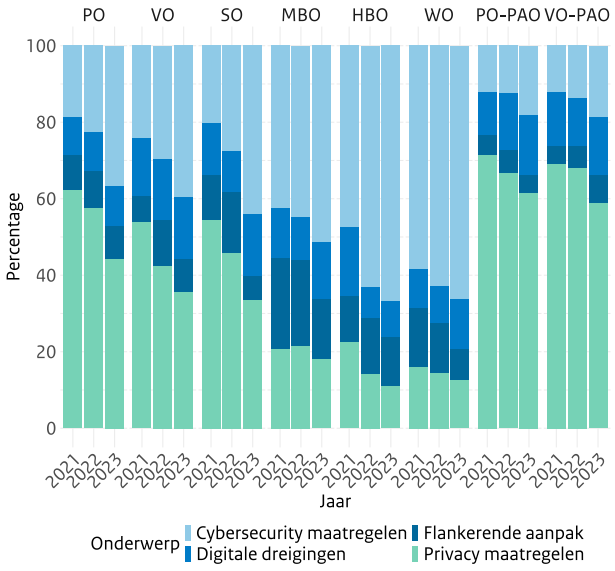


Figuur 3 - *Percentage verantwoording per provincie (2023)*

Analyse van verantwoorde onderwerpen (kwalitatieve analyse)

Omvang verantwoorde onderwerpen digitale weerbaarheid en veiligheid varieert per sector

Onderwijsinstellingen in het funderend onderwijs leggen in hun verantwoording over digitale weerbaarheid en veiligheid de nadruk op privacymaatregelen. In het vervolgonderwijs gaan de verantwoordingen vaker over cybersecuritymaatregelen. De aandacht voor digitale dreigingen en flankerende maatregelen blijft in alle sectoren beperkt. Met andere woorden: incidenten en organisatorische en gedragsverandering blijven onderbelicht in de jaarverslagen. Tegelijkertijd groeit de aandacht voor technische beveiligingsmaatregelen, vooral in het po en so, waar verantwoording hierover sterk toenam sinds 2021. De verschillen tussen verantwoorde onderwerpen hangen vermoedelijk samen met variaties in IT-capaciteit, ervaren verantwoordelijkheid en het strategisch belang van digitale veiligheid.



Figuur 4 - *Verantwoording cybersecurityonderwerpen naar sector*

In dit onderzoek zijn de inspanningen van onderwijsinstellingen op het gebied van digitale weerbaarheid en veiligheid onderverdeeld in 4 hoofdthema's: cybersecuritymaatregelen, privacymaatregelen, flankerende aanpak en digitale dreigingen. Deze classificatie maakt het mogelijk om systematisch in kaart te brengen op welke manieren besturen invulling geven aan hun digitale veiligheid en waar hun accenten in de verantwoording liggen. De hoofdthema's die we gebruiken voor de analyse van de gerapporteerde verantwoordingen zijn in tekstkaders toegelicht.

Cybersecuritymaatregelen

Cybersecuritymaatregelen hebben betrekking op de technische bescherming van IT-systemen. Denk aan het invoeren van tweefactorauthenticatie (of multifactorauthenticatie), 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 welke mate zij aandacht besteden aan het beschermen van hun systemen.

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 kwetsbaarheden waarmee besturen kunnen worden geconfronteerd en de manier waarop zij daarover rapporteren. Het gaat daarbij alleen om incidenten die bij hen plaatsvonden.

Flankerende aanpak

Flankerende aanpak verwijst naar 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.

Privacymaatregelen

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

In 2023 ligt de nadruk in de verantwoording over digitale weerbaarheid en veiligheid in het funderend onderwijs op privacymaatregelen en in het vervolgonderwijs op cybersecuritymaatregelen.
In het po gaat 44% van de verantwoordingen in jaarverslagen over privacymaatregelen, gevolgd door cybersecurity-maatregelen (37%). In het vo liggen privacymaatregelen (36%) en cybersecuritymaatregelen (40%) relatief dicht bij elkaar. In het mbo en ho is het verschil groter: in het mbo gaat 51% van de verantwoordingen over cybersecuritymaatregelen en 20% over privacymaatregelen. In het hbo is dit verschil nog groter, met 67% voor cybersecurity en 11% voor privacy. In het wo is hetzelfde patroon zichtbaar: 66% van de verantwoordingen gaat over cybersecuritymaatregelen, tegenover 12% over privacy.

De nadruk op privacybescherming in het funderend onderwijs kan komen door de gevoeligheid van leerlinggegevens en de aandacht die de AVG daarvoor vraagt. Ook speelt mee dat veel instellingen het technisch beheer uitbesteden, waardoor het besef dat je als organisatie zélf verantwoordelijk blijft voor de beveiliging van je omgeving mogelijk niet altijd voldoende doordringt. In verslaglegging lijkt dit gebrek aan bewust-wording zichtbaar, terwijl bestuurders juist inzicht moeten hebben in risico's om leveranciers goed aan te kunnen sturen. Dit kan een reden zijn dat de normalisering van maatregelen zoals tweefactorauthenticatie trager op gang komt dan in andere onderwijssectoren.

In het vervolgonderwijs is cybersecurity al sinds 2021 het dominante thema. Zoals te zien is in het wo, steeg het aandeel cybersecurity verantwoordingen van 58% naar 66%. In het hbo en mbo is het aandeel cybersecurity verantwoordingen ook gestegen, van 48% naar 67% (hbo) en van 42% naar 51% (mbo). De cijfers laten zien dat instellingen in het vervolgonderwijs nadrukkelijker kiezen voor een technische benadering van digitale veiligheid. Dit kan mogelijk komen door complexere IT-omgevingen, een grotere nadruk op kennisbescherming en de aanwezigheid van gevoelige onderzoeksgegevens. Ook hebben deze instellingen vaker interne IT-afdelingen of gespecialiseerde functionarissen die gericht zijn op het treffen van beveiligingsmaatregelen.

In de jaarverslagen neemt de aandacht voor cybersecuritymaat-regelen toe. Dit lijkt ten koste te gaan van de aandacht voor privacy.
Figuur 4 laat zien dat de aandacht voor cybersecurity-maatregelen in alle onderwijssectoren is toegenomen tussen 2021 en 2023. Vooral in het po, het so en het ho is deze groei opvallend. In het po nam het aantal verantwoordingen toe van 784 in 2021 naar 2.084 in 2023 (+166%). In het so steeg dit aantal van 57 naar 294 (+416%) en in het hbo van 304 naar 582 (+91%). Hoewel de verantwoording over cybersecuritymaatregelen in het po toeneemt, ligt het aandeel verantwoordingen hierover in 2023 (37%) nog onder dat van sectoren als het vo (40%), so (45%), mbo (51%) en ho (ruim 66%). In het so is het aandeel cybersecurityverantwoording relatief hoog, maar het absolute aantal verantwoordingen blijft beperkt door de kleinere omvang van de sector.

In alle sectoren neemt het aandeel verantwoordingen over cybersecuritymaatregelen toe, waarmee dit onderwerp steeds prominenter wordt in de jaarverslagen. Tegelijkertijd is in verschillende sectoren een daling zichtbaar in het aandeel privacymaatregelen. De verantwoording over dit onderwerp neemt niet alleen af in verhouding tot andere maatregelen, maar daalt ook in absolute zin. Ten opzichte van 2021 verantwoordt het vo in 2023 284 keer minder over privacy (–26%) en het po 154 keer minder (–8%). Deze verschuiving kan wijzen op een heroriëntatie van besturen, door toenemende aandacht voor technische beveiligingsmaatregelen. Cybersecuritymaatregelen zijn in het funderend onderwijs minder prominent omdat scholen sterk leunen op de ondersteuning van Kennisnet, SIVON en de Raden. Zij bieden collectief kennis en diensten aan. Hierdoor ligt de focus op bewustwording en basismaatregelen, terwijl zij technische maatregelen vaak centraal of bovenschools regelen en die dus minder zichtbaar zijn in de verantwoordingen.

De aandacht voor digitale dreigingen en flankerende maatregelen in de jaarverslagen is in alle sectoren beperkt, terwijl deze onderwerpen wel belangrijk zijn voor digitale weerbaarheid en veiligheid.
Het onderwerp 'digitale dreigingen' benoemen besturen in alle sectoren relatief weinig, vooral in het funderend onderwijs. In het po gaat slechts 11% van de verantwoordingen over digitale dreigingen, en in het vo is dat 16%. Het so laat een vergelijkbaar beeld zien met 16%. Andere sectoren, zoals het hbo (17%) en wo (13%), scoren iets hoger, maar ook daar blijft het aandeel beperkt. Dit wijst op een bredere trend waarbij besturen dreigingen zoals phishing of ransomware nog onvoldoende expliciet bespreken in jaarverslagen.

De aandacht voor flankerende maatregelen is ook beperkt, met name in het funderend onderwijs. In het po refereert 8% van de besturen in verantwoordingen aan een flankerende aanpak, en in het vo evenveel (8%). In het so ligt dit aandeel zelfs op 6%. Een duidelijke uitzondering vormt het mbo, waar 16% van de besturen verantwoordingen aan dit onderwerp wijdt. Binnen deze aanpak gaat het vooral om bewustwordings-activiteiten en training van personeel. Ook het hbo (13%) en wo (14%) laten meer aandacht zien voor gedragsmatige en organisatorische aspecten, zoals het verantwoorden van structuur en taaktoedeling binnen de organisatie.

De relatief beperkte aandacht voor zowel digitale dreigingen als flankerende aanpak suggereert dat onderwijsinstellingen hun verantwoording vooral richten op concrete maatregelen zoals privacy- en cybersecuritymaatregelen, en minder op risico-inschatting en organisatie- of gedragsverandering. Daarmee blijft een belangrijk deel van digitale weerbaarheid en veiligheid onderbelicht.

Analyse digitale incidenten en datalekmeldingen

Geen duidelijke lijn in gerapporteerde incidenten

Het aantal expliciet gerapporteerde digitale incidenten in onderwijsjaarverslagen blijft beperkt en vertoont schommelingen, zonder duidelijk stijgende of dalende lijn. Vooral in het hoger onderwijs is een toename zichtbaar. Dit komt mogelijk door groeiend bewustzijn en betere meldprocedures. Het is onzeker of de jaarverslagen een volledig beeld geven van de werkelijke aantallen, maar openheid over incidenten kan juist helpen om van elkaar te leren en het stelsel als geheel sterker te maken.

De ontwikkeling van het aantal gerapporteerde incidenten in de jaarverslagen vanaf 2021 tot en met 2023 varieert per onderwijssector. Binnen het po nam het aantal gerapporteerde incidenten af van 94 in 2021 naar 65 in 2022, gevolgd door een stijging naar 78 in 2023. Specifiek het aantal beveiligingsincidenten binnen deze sector nam in 2023 toe ten opzichte van 2022. In het vo daalde het aantal incidenten ook, van 73 in 2021 naar 58 in 2022, waarna een lichte stijging naar 59 werd waargenomen in 2023. In het mbo was sprake van een voortdurende daling: van 29 incidenten in 2021 naar 20 in 2022 en verder naar 19 in 2023. In het ho is daarentegen een stijgende trend zichtbaar: van 18 incidenten in 2021 naar 26 in 2023. Deze stijging in het aantal gerapporteerde incidenten ligt in een toename van het aantal datalekken en gemelde cyberaanvallen.

De gegevens tonen geen verband tussen de dreiging en impact van verschillende typen incidenten. Hoewel het aantal gemelde incidenten per sector schommelt, is er geen duidelijke lijn te ontdekken die wijst op een structurele toename of afname. Tegelijkertijd kan een toename in het aantal gemelde incidenten, zoals zichtbaar in het ho, ook duiden op een grotere interne bewustwording. Werknemers zijn mogelijk beter in staat incidenten zoals phishingpogingen of datalekken te herkennen en melden deze sneller bij de FG of via een interne meldingsprocedure van het bestuur.

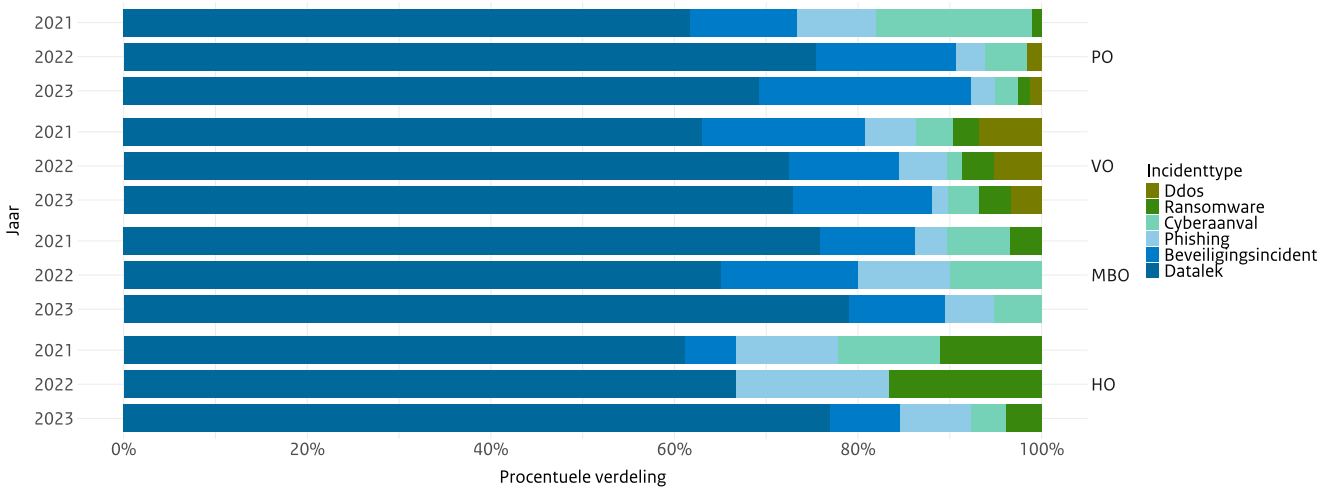
De stap om deze meldingen vervolgens te verantwoorden in het jaarverslag is een ander verhaal. De mate waarin besturen zich publiekelijk verantwoorden over incidenten verschilt sterk per bestuur. Het is dus onzeker of de jaarverslagen een volledig beeld geven van de werkelijke aantallen. Mogelijk bestaat er een verschil in inschatting van de relevantie van een incident. Ook kan er sprake zijn van bewuste terughoudendheid om incidenten expliciet te rapporteren. Besturen kunnen bijvoorbeeld vrezen voor imagoschade of het risico dat zij hierdoor juist meer als doelwit worden gezien. Dit maakt het lastig om een volledig en eerlijk beeld te krijgen van de werkelijke aantallen. Tegelijkertijd kan openheid over incidenten, in verschillende vormen van kennisdeling, helpen om van elkaar te leren en het stelsel als geheel sterker te maken.

Gerapporteerde dreigingen hebben meestal een interne oorzaak

In alle onderwijssectoren blijkt het merendeel van de digitale incidenten in 2023 veroorzaakt te zijn door interne factoren, zoals menselijke fouten of onzorgvuldig gegevensgebruik. Vooral in het po en mbo is een sterke stijging zichtbaar in het aandeel interne dreigingen sinds 2021, wat kan duiden op zowel verhoogde meldingsbereidheid als structurele kwetsbaarheden binnen interne processen. Dit onderstreept het belang van organisatorische maatregelen naast technische beveiliging.

Interne dreigingen zijn bijvoorbeeld datalekken door menselijke fouten, onzorgvuldig gebruik van persoonsgegevens of incidenten binnen de eigen beveiliging. Externe dreigingen gaan onder meer over cyberaanvallen of phishing. Dit onderscheid helpt beter te begrijpen waar de grootste kwetsbaarheden liggen en hoe deze zich over de jaren ontwikkelen.

De meerderheid van de gerapporteerde incidenten in 2023 is veroorzaakt van binnenuit. In het po was 87% van de incidenten intern van aard (68 van de 78). In het vo ging het om 83% (49 van de 59), in het mbo om 95% (18 van de 19) en in het ho om 85% (22 van de 26). Sinds 2021 is vooral in het po een duidelijke verschuiving zichtbaar: het aandeel interne dreigingen steeg van 61% naar 87%. In het vo nam dit aandeel toe van 77% naar 83%. Het mbo liet een vergelijkbare stijging zien, van 83% naar 95%. Ook in het hoger onderwijs nam het aandeel interne incidenten merkbaar toe: van 70% in 2021 naar 85% in 2023.



Figuur 5 - *Relatieve verdeling van incidenttypen per sector en jaar*

De data laten zien dat een groot deel van de gerapporteerde incidenten voortkomt uit interne gebeurtenissen. Dat is deels verklaarbaar: vaak zijn datalekken in het po het gevolg van interne fouten, zoals een e-mail met leerlinggegevens die iemand per ongeluk naar de verkeerde ontvanger stuurt. Binnen het po is veel aandacht voor de AVG en medewerkers zijn zich sterk bewust van privacyregels. Daardoor worden dit soort incidenten sneller opgemerkt en gemeld. Het gaat vaak om kleine schoolbesturen die werken met gevoelige informatie van jonge kinderen, wat de alertheid vergroot.

Opvallend is daarnaast de sterke toename van interne dreigingen binnen het mbo. Mogelijke verklaringen zijn een groeiend bewustzijn en verbeterde meldprocedures, maar het kan ook wijzen op structurele kwetsbaarheden in interne processen.

Meldingen bij de Autoriteit Persoonsgegevens variëren per sector

Onderwijsinstellingen verschillen sterk in hun meldgedrag bij de Autoriteit Persoonsgegevens (AP), met het laagste aandeel in het po en hogere meldingsgraad in het vo, mbo en ho. De lage mate van expliciete AP-meldingen in het po wijst op beperkte transparantie of afwezigheid van systematische toelichting in jaarverslagen.

Een melding bij de AP is alleen verplicht wanneer het incident mogelijk impact heeft op de privacy van betrokkenen. Wanneer die impact ontbreekt, kunnen besturen besluiten om geen melding te doen. De cijfers geven daarmee inzicht in de ernst waarmee instellingen hun incidenten inschatten én in de mate waarin zij bereid zijn deze te melden bij de AP.

In 2023 meldden instellingen gemiddeld 40% van de in jaarverslagen gerapporteerde incidenten ook daadwerkelijk bij de AP. Dit percentage baseren wij op zelfrapportage van besturen in de jaarverslagen en wijkt af van het werkelijke aantal meldingen dat bij de AP zelf geregistreerd staat. Instellingen meldden 32% van de incidenten bewust niet, en bij 28% van de verantwoordingen lichtten zij deze niet toe. In het vo meldden instellingen 55% van de incidenten (32 van de 58), in het mbo 58% (11 van de 19) en in het ho 65% (13 van de 20). In het po ligt dit aandeel op 30% (23 van de 78 incidenten). Dit hoeft alleen niet te betekenen dat deze besturen minder zorgvuldig handelen: het kan erop wijzen dat zij incidenten vaak als niet-meldplichtig inschatten. Belangrijk is vooral dat besturen transparant zijn over hoe zij de afweging maken om een incident wel of niet bij de AP te melden.

In de jaarverslagen komt ook niet altijd duidelijk naar voren of het bestuur een incident meldde. In het po is het aandeel ‘onbekend’ relatief hoog (31%, 24 van de 78 incidenten). ‘Onbekend’ betekent dat het schoolbestuur in het jaarverslag niet beschreef of zij het incident meldde. Dat sluit een daadwerkelijke melding niet uit.

Ten opzichte van 2021 is het aantal meldingen in het vo gestegen van 24 naar 32. In het ho ging het van 10 naar 13. Het po laat juist een daling zien: van 30 gemelde incidenten in 2021 naar 23 in 2023. Tegelijk is daar het aantal ‘onbekend’ gestegen van 17 naar 24. Hoewel besturen gemiddeld ruim 40% van de incidenten melden bij de AP, is dit voor het po niet het geval. Mogelijk beoordelen besturen incidenten daar vaker als niet-meldplichtig, of ontbreekt het aan systematische toelichting in de jaarverslagen. Het relatief hoge aandeel ‘onbekend’-meldingen suggereert bovendien terughoudendheid om hierover transparant te zijn.

Wat zegt de Autoriteit Persoonsgegevens hierover?

Behoefte aan structurele basis in privacybeleid
De Autoriteit Persoonsgegevens (AP) constateert dat de onderwijssector zich over het algemeen positief ontwikkelt op het gebied van privacy, maar dat de basis in veel instellingen nog niet op orde is. Hoewel er steeds vaker beleid op papier staat, blijft de praktische uitvoering achter. Bijvoorbeeld door gebrekkige meldprocedures bij datalekken of onvoldoende formatieruimte voor privacyprofessionals. Vooral kleinere instellingen hebben moeite om structurele privacymaatregelen te implementeren, mede door beperkte capaciteit en kennis.

Sterke opkomst van collectieve ondersteuning
In alle sectoren, maar met name in het mbo en ho, is een duidelijke toename zichtbaar in samenwerking rond informatiebeveiliging en privacy. Via SURF, SIVON en MBO Digitaal worden DPIA’s, verwerkersovereenkomsten en risicoanalyses op centraal niveau georganiseerd. Ook het funderend onderwijs kent gemeenschappelijke initiaven om digitaal veiliger te werken. Denk hierbij aan het programma Digitaal Veilig Onderwijs. Dit soort initiatieven zijn belangrijk om (met name) de lasten van kleine onderwijsinstellingen te verminderen.

Nieuwe risico’s
De AP signaleert nieuwe risico’s die het onderwijsveld onder druk zetten: de opkomst van algoritmes en AI vraagt om nieuwe beleidskaders, terwijl het ongecontroleerd gebruik van apps en tools (schaduw-IT) het zicht op gegevensverwerkingen vertroebelt. Bovendien worden veel persoonsgegevens onnodig bewaard in verouderde systemen. Dit draagt bij aan onnodige risico’s bij datalekken of cyberaanvallen. In 2022 ontving de AP ruim 700 datalekmeldingen vanuit de onderwijssector, goed voor ongeveer 3% van alle Nederlandse datalekmeldingen (de inspectie vond in totaal 71 gerapporteerde AP-meldingen in de jaarverslagen). Gezien het grote aantal instellingen (meer dan 7.000) en betrokkenen (ruim 4 miljoen) vindt de AP dit een opvallend laag cijfer. De AP roept instellingen daarom op om actiever werk te maken van dataminimalisatie en privacybewuste digitale keuzes. Juist omdat het onderwijs bij uitstek een sector is waarin vertrouwen en bescherming van kwetsbare groepen centraal moeten staan.

Autoriteit Persoonsgegevens. (2024, 24 januari). Sectorbeeld Onderwijs 2021–2023. Sectorbeeld Onderwijs 2021-2023 | Autoriteit Persoonsgegevens

De noodzaak van digitale weerbaarheid

Digitale dreiging niet meer weg te denken

Digitale incidenten bij Nederlandse onderwijsinstellingen komen steeds vaker voor. Een digitaal incident kan grote gevolgen hebben voor onderwijscontinuïteit, privacy en vertrouwen. De hack bij de TU Eindhoven begin 2025 en de datadiefstal bij leverancier Iddink in 2024 trokken veel aandacht in de media, maar de afgelopen jaren werden meerdere instellingen in het po, vo, so en mbo getroffen. Dergelijke incidenten onderstrepen het belang van structurele aandacht voor weerbaarheid, transparantie en digitale verantwoordelijkheid binnen het onderwijs. Ook de inspectie plaatst dit onderwerp hoog op de agenda. De komende jaren blijft zij dit onderwerp monitoren. De jaarverslagen 2024 vormen onderwerp van analyse voor de Monitor 2025.

Digitale weerbaarheid is een bestuurlijke opdracht

Besturen moeten zich realiseren dat het waarborgen van digitale veiligheid essentieel is om vandaag en in de toekomst goed onderwijs voor elke leerling en student te kunnen blijven verzorgen.
Bij digitale weerbaarheid gaat het wat de inspectie betreft in de kern om het waarborgen van 4 basisprincipes:

- de continuïteit van het onderwijs;
- beschikken over correcte persoonsgegevens zodat passende leerlijnen kunnen worden geboden;
- integriteit van onderwijsdata zodat de waarde van het diploma niet in geding komt;
- rechtmatige besteding van bekostiging.

Elk bestuur moet hiernaar handelen, passend bij het eigen risicoprofiel.

Aan de slag met digitale weerbaarheid en veiligheid?

Bekijk onze factsheet 'Binnen Zonder te Kloppen' voor een samenvatting waarin wij bestuurders van alle onderwijsinstellingen en uit alle onderwijssectoren op een laagdrempelige manier informeren en hen helpen om over te gaan tot actie.

Noodzaak van goede verantwoordingen over digitale veiligheid en weerbaarheid in het jaarverslag

Het jaarverslag biedt de ruimte om te laten zien hoe een bestuur aan digitale weerbaarheid en veiligheid werkt en welke resultaten zij behaalt. De Monitor digitale weerbaarheid en veiligheid 2021-2023 van de inspectie laat zien dat de omvang en de diepgang van de verantwoordingen over dit onderwerp jaarlijks toenemen en dat steeds meer besturen maatregelen nemen om hun digitale weerbaarheid te versterken. De bedoeling is dat op korte termijn alle besturen in alle sectoren zich in het jaarverslag over dit onderwerp gaan verantwoorden. Een goede verantwoording laat aan de belanghebbenden van een bestuur zien hoe het bestuur zijn verantwoordelijkheid op het vlak van digitale weerbaarheid en veiligheid invult. De inspectie verwacht van besturen niet alleen dat ze open zijn over hun aanpak maar ook over hun uitdagingen. Een goede verantwoording betekent namelijk niet dat besturen alles al perfect hebben geregeld, maar dat zij transparant delen waar zij staan in termen van successen en leerpunten. Transparantie komt het hele veld ten goede: hoe meer besturen laten zien hoe zij omgaan met digitale dreigingen, hoe meer andere besturen hiervan kunnen leren.

Verantwoording als sluitstuk van de planning- en controlcyclus

Verantwoording volgt op inhoudelijk handelen. Het is geen doel op zich, maar een manier om de voortgang zichtbaar te maken en te monitoren. Een goede verantwoording vormt het sluitstuk van een complete planning- en controlcyclus (P&C-cyclus), waarin plannen, acties en evaluaties elkaar opvolgen. Het onderwerp digitale weerbaarheid en veiligheid verdient een eigen plaats in de P&C-cyclus van een bestuur. Dit betekent dat een bestuur nadenkt over zijn eigen risico's op dit vlak en een beleid formuleert waarin staat hoe de instelling deze risico's beheerst. Ook volgt het bestuur de acties die hieruit voortkomen en stuurt bij als dat nodig is. Het bestuur evalueert periodiek de effectiviteit van de acties, de monitoring én het beleid. Het ligt voor de hand om digitale weerbaarheid en veiligheid als risicocategorie op te nemen in de periodieke risicoanalyse en bovengenoemde activiteiten onderdeel te maken van het risicobeheersingssysteem.

Maak gebruik van tools van Kennisnet, Sivon en SURF

Kennisnet ontwikkelde een tool voor schoolbesturen in het po, vo en so om aan de slag te gaan met het Normenkader Informatiebeveiliging en Privacy Funderend Onderwijs.

Het Security Expertise Center van SURF biedt het vervolgonderwijs op deze thema's veel informatie die besturen kunnen helpen regie te pakken op digitale veiligheid.

Basisprincipes van digitale weerbaarheid van het Nationaal Cyber Security Centrum

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.

Colofon

Foto voorpagina: Bert Kasteel

Inspectie van het Onderwijs
Postbus 2730 | 3500 GS Utrecht
www.onderwijsinspectie.nl

Een exemplaar van deze publicatie is te downloaden van de website van de Inspectie van het Onderwijs. Op de website vindt u ook het technisch rapport dat bij dit onderzoek hoort.