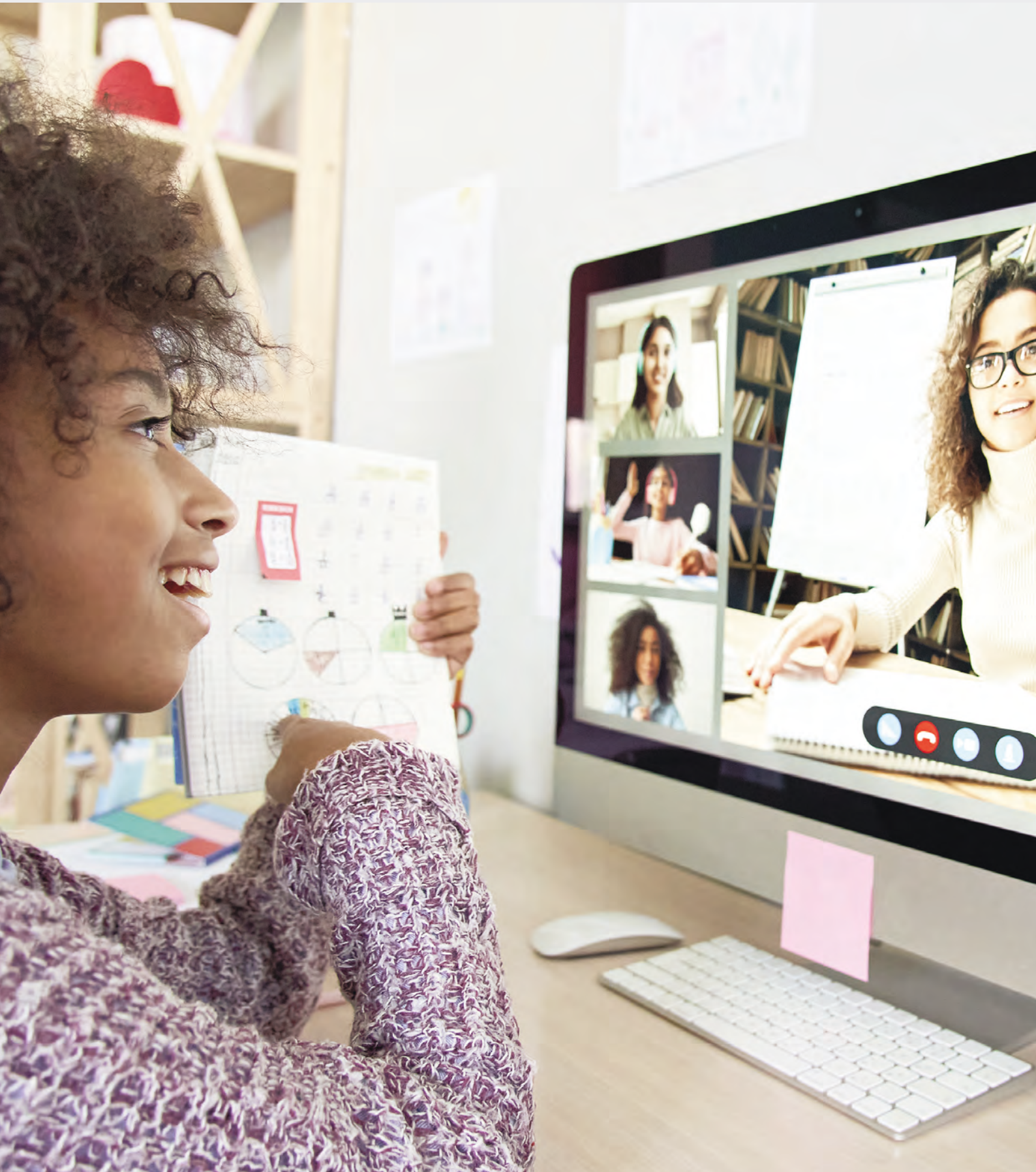
Auteur: Jordy van den Elshout MSc CISSP, de CISO van Kennisnet. Hij is bereikbaar via: j.vandenelshout@kennisnet.nl.



Eenduidige beveiliging van onderwijstoepassingen essentieel voor een digitaal veilig onderwijs

Elke leerling moet kunnen leren in een digitaal veilige schoolomgeving. Dat betekent dat ICT-toepassingen die docenten en leerlingen gebruiken, veilig moeten zijn. Zij mogen ervan uitgaan dat hun persoonsgegevens voldoende beschermd zijn. Maar wat is veilig genoeg? En is het beveiligingsniveau dat een leverancier biedt voldoende? Om deze vragen te beantwoorden is het Certificeringschema IBP ontwikkeld. Hierin is overeenstemming bereikt over het (basis)niveau van informatiebeveiliging en privacy van onderwijstoepassingen.

Net als in onze maatschappij speelt digitalisering een grote rol in het onderwijs. Al lange tijd worden ICT-toepassingen gebruikt, in plaats van enkel boeken. Ook toetsen worden steeds vaker via de computer afgenomen. Dat zie ik ook bij mijn dochters op de basisschool gebeuren. Deze verandering biedt voordelen, maar brengt ook risico's met zich mee. Het leidt tot vraagstukken rondom het verzamelen van gevoelige gegevens van kinderen. Uitlekken van deze gegevens kan namelijk grote gevolgen hebben. Daarnaast worden we steeds afhankelijker van digitale middelen, waardoor de beschikbaarheid van onderwijstoepassingen belangrijker wordt. Vooral op cruciale momenten. Bijvoorbeeld wanneer een toets gepland staat waar leerlingen zich lange tijd op voorbereid hebben. Wanneer de toets niet beschikbaar is door een verstoring, leidt dat tot vervelende situaties. En nog vervelender is het als de uitslagen voor de toets onjuist zijn omdat de integriteit van de toepassing onvoldoende geborgd is.

Om deze digitale onderwijstoepassingen adequaat en naar wens van het onderwijs te beveiligen, zijn afspraken nodig. Het belang van een toepassing voor het onderwijs kan namelijk het beste door het onderwijs zelf bepaald worden; de afnemer van de onderwijstoepassing. Daarom zijn er afspraken gemaakt over hoe dit belang bepaald moet worden en welk beveiligingsniveau daarbij hoort. Dit is uitgewerkt in het Toetsingskader van het Certificeringschema IBP.

> Het Certificeringschema IBP is onderdeel van de Referentie Onderwijs Sector Architectuur (ROSA) (1), een vastgestelde afspraak binnen Edustandaard. Edustandaard is het platform waar alle publieke en private partijen binnen het onderwijsveld bij elkaar komen om afspraken te maken, te beoordelen en vast te stellen. Vanuit Kennisnet begeleid ik de Werkgroep IBP (2) die het Certificeringschema IBP onderhoudt. Deze afspraak is opgesteld om ICT-toepassingen in het onderwijs te toetsen. In een apart document Toezicht wordt dit nader uiteengezet. Voor dit artikel beperk ik de toelichting tot de inhoud van het Certificeringsschema: het Toetsingskader.

Maatregelen

In het Toetsingskader is een eenduidig (basis)niveau van informatiebeveiliging en privacy bepaald. Het geeft beveiligingseisen

voor een onderwijstoepassing, verdeeld over drie categorieën: beschikbaarheid, integriteit en vertrouwelijkheid (BIV).
Op basis van de BIV-classificatie worden de minimale beveiligingsmaatregelen voorgeschreven, zodat de onderwijstoepassing afdoende wordt beveiligd volgens het belang voor de beschikbaarheid, integriteit en vertrouwelijkheid. Dit voorkomt onnodig zware beveiligingsmaatregelen, die ten koste gaan van het budget of van de gebruikersvriendelijkheid. Maar zorgt ook voor voldoende zware maatregelen als het onderwijsproces of de gebruikte gegevens dat vereisen. Hoe deze classificatie bepaald wordt, licht ik later toe.

Om een beeld te geven van een maatregel op basis van het BIV-niveau: wanneer de beschikbaarheid van een onderwijstoepassing minder van belang is en daardoor een laag niveau voor beschikbaarheid kent, mag deze bijvoorbeeld bestaan uit enkele applicatieonderdelen. Maar wanneer de toepassing een hoog beschikbaarheidsniveau kent, dan worden dubbele applicatieonderdelen voorschreven. Dit kan ingevuld worden met meerdere servers in combinatie met een 'load-balancer'.

Voor de vertrouwelijkheid geldt hetzelfde. Wanneer een onderwijstoepassing een laag vertrouwelijkheidsniveau kent, bijvoorbeeld het inzien van het schoolrooster, dan is geen tweefactorauthenticatie (2FA) vereist. Maar bij een onderwijstoepassing met gevoelige persoonsgegevens van leerlingen is toegang met 2FA wel verplicht.

Vaststellen juiste BIV-classificatie van belang

Afdoende beveiliging valt of staat met een goede inschatting van de BIV-classificatie. Wanneer deze niet juist wordt ingeschat, leidt dit tot te lichte of te zware maatregelen op het gebied van beschikbaarheid, integriteit of vertrouwelijkheid. Daarom is een classificatieschema onderdeel van het Toetsingskader, in de vorm van een vragenlijst. De vragenlijst geeft een objectieve indicatie voor de BIV-classificatie.

Voor de beschikbaarheid wordt bijvoorbeeld de volgende vraag gesteld: welke impact heeft uitval (de data, informatie of ICT-toepassing zijn niet beschikbaar)? Mogelijke antwoorden hierop zijn: a) geen; b) het proces wordt belemmerd maar kan wel doorgaan; of c) het proces kan in zijn geheel niet doorgaan. Op basis van meerdere antwoorden in de categorie beschikbaarheid wordt het niveau bepaald: laag, midden of hoog. Op dezelfde manier wordt het niveau bepaald voor integriteit en vertrouwelijkheid. Een van de vragen voor vertrouwelijkheid is: kunnen personen schade ondervinden als gevolg van het uitlekken van de gegevens?

Met deze vragen wordt een link gelegd met het proces en de benodigde informatie, waar het in informatiebeveiliging om te doen is. De applicatie wordt daarmee in de juiste context geplaatst. Door een link te leggen met het proces, kan je het belang van beschikbaarheid en integriteit bepalen. Op basis hiervan wordt ook de hersteltijd (Recovery Time Objective) en maximale dataverlies in uren (RPO) aangewezen. Door naar de gebruikte informatie te kijken, kan je de gevoeligheid ervan bepalen, ofwel de vertrouwelijkheid.

> Als vragen in het Classificatieschema verkeerd geïnterpreteerd en beantwoord worden, kan dat leiden tot een onjuiste BIV-classificatie. Daarom wordt door de Werkgroep IBP van Edustandaard ook gekeken naar een aanvullende afspraak: een koppeling met referentiearchitectuur in het onderwijs, waarin BIV-classificatie van soorten applicaties centraal vastgesteld worden. Dit leidt tot meer uniformiteit in de BIV-classificatie en verkleint de kans op discrepantie en discussie.

Complementair aan andere normenkaders

Het Toetsingskader is een (nadere) aanvulling op normenkaders voor informatiebeveiliging, zoals de ISO 27001/2 en NIST SP 800-53. Maar ook op de normenkaders voor informatiebeveiliging en privacy die in het onderwijs gehanteerd worden, die gebaseerd zijn op het NBA-volwassenheidsmodel (3). Al deze normen richten zich met name organisatiebreed en niet specifiek op een onderwijstoepassing, zoals het Toetsingskader van het Certificeringschema IBP ROSA dat wel doet. Hierdoor is het Toetsingskader complementair aan eerdergenoemde normenkaders.

Leveranciers van onderwijstoepassingen gebruiken vaak al een normenkader voor informatiebeveiliging. Zij kunnen het Toetsingskader als aanvulling gebruiken. Het classificatieschema kan gebruikt worden om de onderwijstoepassing te classificeren. Vervolgens kunnen per applicatie passende maatregelen genomen worden, zoals in het begin van dit artikel uitgelegd.

Bij Kennisnet gebruiken we het Toetsingskader ook als aanvulling op ons ISMS volgens ISO 27001. Aangezien wij voor de landelijke

Om de digitale onderwijstoepassingen adequaat en naar wens van het onderwijs te beveiligen, zijn afspraken nodig

ICT-basisinfastructuur voor het primair- en voortgezet onderwijs en het mbo een breed scala aan diensten leveren (4), hebben wij voor het overzicht al onze diensten en onderliggende applicaties vastgelegd in een administratiesysteem. De vragenlijst van het classificatieschema voor het vaststellen van de BIV is hier onderdeel van en wordt door dienstverantwoordelijken ingevuld. Op basis van de BIV-classificatie worden de juiste beveiligingseisen geselecteerd en kan per maatregel de status bijgehouden worden. Op deze wijze houden we grip op en inzicht in de beveiligingseisen die per dienst decentraal geborgd moeten worden.

Kennisnet is de publieke organisatie (5) voor ICT in het primair- en voorgezet onderwijs en voor specifieke thema's in het mbo. Kennisnet zorgt ervoor dat technologie wordt benut om de kwaliteit en toegankelijkheid van het onderwijs te verbeteren en veiligheids- en ICT-risico's te beheersen. Hiervoor neemt Kennisnet verschillende rollen aan:

i) **Expert en gids** voor scholen en besturen die keuzes moeten maken over inzet van ICT,
ii) **Ontwikkelaar en dienstverlener** van publieke ICT-voorzieningen, en
iii) **Keten- en sectorarchitect** van de (sectorale en bovensectorale) ICT-infrastructuur in het onderwijs.

Kennisnet geeft ook advies over toepassing van informatiebeveiliging en privacy (IBP). Hiervoor is o.a. de Aanpak IBP (6) ontwikkeld, waar ook het Normenkader IBP op beschikbaar is gesteld. Ook werkt Kennisnet samen met andere publieke partijen om IBP in het onderwijs op een hoger niveau te krijgen. Hiervoor is het Programma Digitaal Veilig Onderwijs (7) gestart, met ministerie van OCW als opdrachtgever.

Beveiliging van de toepassing zelf

Wanneer je meer zekerheid wilt over de toegepaste informatiebeveiliging, dan vraag je daar bewijs van op. Als een leverancier ISO 27001 gecertificeerd is, vraag je het certificaat op, inclusief de 'Verklaring van Toepasselijkheid' (VvT). Het certificaat maakt inzichtelijk of de processen voor informatiebeveiliging volgens de norm (ISO 27001) zijn ingericht en op welk deel van de organisatie ('scope').

In de VvT staat beschreven welke maatregelen wel of niet van toepassing zijn, en waarom. Hier kun je nog op doorvragen, bijvoorbeeld op welke wijze de maatregelen zijn ingevuld. Logischerwijs stel je de vragen op basis van een eigen risicoanalyse voor jouw situatie.

Op dat moment heb je meer zicht en zekerheid over de processen die op organisatieniveau georganiseerd zijn, echter zegt dit weinig over de beveiligingseigenschappen van de geleverde onderwijstoepassing zelf. Dat inzicht is wel wenselijk, vooral als een leverancier geen ISO 27001 certificering heeft. Het Toetsingskader kan dit inzicht leveren op basis van de gewenste BIV-classificatie.
De leverancier kan het Toetsingskader invullen voor een specifieke onderwijstoepassing die zij leveren. Hierin kunnen zij de vragen beantwoorden die leiden tot een BIV-classificatie voor beoogd gebruik. Vervolgens kan per maatregel aangegeven worden wat de status is, inclusief toelichting. De onafhankelijkheid wordt bepaald door de toetsvorm, ofwel door wie de toets is uitgevoerd. Binnen het Certificeringsschema onderkennen we vier toetsvormen:

1. Self-assessment (lage onafhankelijkheid)
2. Interne audit (gemiddelde onafhankelijkheid)
3. Peer review (gemiddelde onafhankelijkheid)
4. Externe audit (hoogste onafhankelijkheid)

Hiermee heb je inzicht in het beveiligingsniveau van de toepassing zelf en in hoeverre dit is toegepast. Mocht het niveau onvoldoende blijken voor het gebruik, dan kun je hier extra eisen

Maak gebruik van het Certificeringschema!
Het Certificeringschema ROSA IBP is ontwikkeld voor het onderwijs, maar ook zeker toepasbaar voor andere sectoren of binnen een organisatie zelf, zoals Kennisnet dat ook doet. Het is vrij te gebruiken (CC-BY) en te downloaden via de website van Edustandaard.

aanstellen. Mocht je meer zekerheid willen over de toepassing van de maatregelen, dan kun je de toets laten uitvoeren door een externe auditor.

Borgen van beveiligingseisen

Het Toetsingskader zorgt ook voor het specificeren van de adequate beveiligingseisen in een verwerkersovereenkomst. Deze omvat vaak een standaardlijst met beveiligingseisen, maar de AVG vereist dat er passende maatregelen worden genomen. Met de BIV-classificatie kun je aangeven wat gewenst en passend is. Op basis van het toetsingskader kunnen dan de specifieke beveiligingseisen voor dat niveau voorgeschreven worden in de beveiligingsbijlage. Tijdens een DPIA kan een ingevuld Toetsingskader opgevraagd worden, om toepassing van deze beveiligingseisen te controleren.

In de modelverwerkersovereenkomst (van het Privacy Convenant (8)) voor het primair- en voorgezet onderwijs en het mbo wordt het Toetsingskader daarvoor ook gebruikt. Het Toetsingskader (Excelsheet) heeft daar speciaal een rapportfunctie voor, dat een-op-een overgenomen kan worden in de beveiligingsbijlage van een verwerkersovereenkomst. Daarmee worden de beveiligingsmaatregelen ook contractueel geborgd.

Referenties

(1) https://rosa.wikixl.nl
(2) https://www.edustandaard.nl/standaard_werkgroepen/werkgroep-informatiebeveiliging-en-privacy-ibp
(3) https://www.nba.nl/tools-en-ondersteuning/publicaties/2019/handreiking-bij-volwassenheids-model-informatiebeveiliging/
(4) https://www.kennisnet.nl/diensten
(5) Kennisnet wordt gefinancierd door het ministerie van Onderwijs, Cultuur en Wetenschap (OCW)
(6) https://aanpakibp.kennisnet.nl/normenkader/
(7) https://www.digitaalveiligonderwijs.nl/
(8) https://www.privacyconvenant.nl/downloads/