AON

onderWIJS
magazine

Versterken van je digitale verdediging

1

Voorwoord

Beste lezers,

Het nieuwe onderwijsjaar is van start gegaan, een tijd vol nieuwe kansen en uitdagingen. Terwijl de deuren zijn geopend voor de (nieuwe) leerlingen, studenten en nieuwe collega's, worden ze verwelkomt in een wereld die voortdurend verandert. Het is daarom cruciaal dat er binnen de onderwijsinstellingen aandacht wordt besteed aan cyberweerbaarheid, gelukkig is dit een onderwerp dat steeds meer prioriteit krijgt.

In deze editie van OnderWIJS richten we ons op het versterken van de digitale verdediging. We bespreken het belang van risicomanagement en Incidentresponse-management en hoe we ons kunnen voorbereiden op mogelijke cyberaanvallen. Ook belichten we preventieve maatregelen en wat deze betekent voor onderwijs-instellingen, inclusief de verplichtingen en kansen die het met zich meebrengt.

Het managen van een crisis is een andere belangrijke pijler. We geven u alvast een sneak preview over strategieën en trainingen om effectief te reageren in het geval van een crisis en daarmee de continuïteit van uw onderwijsinstelling te waarborgen. Daarnaast presenteren we innovatieve cyberoplossingen die kunnen helpen om de onderwijsinstellingen te beschermen en de veiligheid van jullie gegevens te garanderen.

Last but not least delen Gert van Millingen en Cyro van Malsen van Nuovo scholen waardevolle inzichten en tips over de keuzes en weerstanden die zijn overwonnen bij het verhogen van de cyberweerbaarheid.

Laten we deze nieuwe kansen grijpen en proactief de risico's beheersen. Samen bouwen we aan een veilig en veerkrachtig onderwijslandschap voor de toekomst.

Een succesvol en veilig nieuw schooljaar gewenst!

Harm & Henri

Harm Mulder
Practice Leader Education

Henri Damen
Account Executive

De waarde van risicomanagement en Incident Response Management

Cyberweerbaarheid is cruciaal voor onderwijsorganisaties. Of u nu wilt voldoen aan het Normenkader of voorbereid wilt zijn op de nieuwe cyberwet NIS2, preventieve maatregelen volgens het NIST-framework zijn essentieel om de kans op een cyberincident te verkleinen. Maar wat doet u als deze maatregelen falen en er een 'cyberbrand' uitbreekt?

Lees verder ›

Wat is uw plan?

Hoewel onderwijsinstellingen momenteel niet hoeven te voldoen aan de NIS2-richtlijn, moeten PO- en VO-scholen in 2027 wel voldoen aan het Normenkader. Dit kader biedt richtlijnen voor informatiebeveiliging, en als schoolbestuurder bent u eindverantwoordelijk voor de implementatie. De toenemende cyberdreigingen en de complexiteit van digitale beveiliging kunnen overweldigend zijn.

Dit artikel bespreekt risicomanagement en Incidentresponse-management en hoe deze bijdragen aan het voldoen aan 'streefniveau 3' van het Normenkader. De uitdagingen en oplossingen voor PO en VO zijn ook relevant voor MBO, HBO en universiteiten. Bovendien wordt ingegaan op situaties waarin preventieve maatregelen falen.

De urgentie van een plan

Risicomanagement is een cruciaal onderdeel van het Normenkader en van een gedegen cyberweerbaarheidsplan. Het gaat niet alleen om het identificeren van risico's, maar ook om het ontwikkelen van een aanpak om deze te beheersen. Aon helpt bij het opstellen van een raamwerk voor informatierisicomanagement dat aansluit bij de doelstellingen van uw organisatie. Zo blijft uw organisatie voorbereid op verstoringen en beheersbaar voor risico's.

Incident Response Management is minstens zo belangrijk. Een effectief incidentmanagementproces zorgt ervoor dat incidenten snel worden gedetecteerd, geïsoleerd en opgelost, zodat de impact minimaal is. Aon ondersteunt bij het opstellen van een incidentmanagementbeleid, inclusief escalatieprocedures en responsplannen, zodat uw organisatie goed voorbereid is op incidenten en adequaat kan handelen wanneer dat nodig is.

Daarnaast biedt Aon een Incident Response Service als directe hulplijn bij incidenten en crises. Deze dienst, los van een cyberverzekering, geeft u 24/7 toegang tot deskundige begeleiding, coördinatie en hulp bij noodsituaties. Hierdoor kunt u effectief reageren en schade beperken, en voldoet u beter aan het Normenkader of NIS2.

Lees ook het interview met Hector Hamaker over Incident Response.

Lees verder >

Blijvend risico op financiële schade

100% cyberveiligheid is een utopie. Zelfs na het implementeren van het Normenkader, NIS2 of het NIST-framework, blijft er een risico op financiële schade door een cyberincident. Een cyberverzekering maakt uw organisatie niet cyberveilig, maar biedt bescherming tegen de financiële gevolgen van een hack, lek of aanval, waaronder ransomware.

Waarom Aon?
Aon combineert diepgaande kennis van het onderwijs met expertise in risicomanagement en cybersecurity. Onze integrale aanpak zorgt ervoor dat uw organisatie niet alleen voldoet aan het Normenkader, maar ook voorbereid is op toekomstige cyberdreigingen. We ondersteunen u bij elke stap, van risicobeoordeling en implementatie van maatregelen tot het afdekken van financiële risico's met een cyberverzekering.

Bent u klaar voor 2027?
Neem vandaag nog contact op met Aon om te bespreken hoe wij uw organisatie kunnen helpen voldoen aan het Normenkader en uw cyber-weerbaarheid kunnen verhogen.

Samen maken we het onderwijs cyberveiliger.

Het is belangrijk te benadrukken dat Aon en cybersecurityexperts niet de rol van uw ICT-partner overnemen, maar juist samenwerken om te kunnen voldoen aan het Normenkader, ieder vanuit de eigen verantwoordelijkheid en expertise. Dit zorgt voor een geïntegreerde aanpak waarbij uw organisatie optimaal wordt ondersteund op alle fronten.

Een cyberincident ... en dan?

Als er op dit moment een cyberincident plaatsvindt, wat doet u dan?

Door de toenemende digitalisering binnen het onderwijs wordt de bescherming van gevoelige gegevens en IT-infrastructuren voor onderwijsinstellingen steeds belangrijker. In de krant zien we regelmatig dat basisscholen, middelbare scholen, hogescholen en universiteiten slachtoffer zijn geworden van een cyberincident, zoals een hack of datalek. “Het is tegenwoordig niet meer de vraag óf, maar wanneer je geraakt wordt door cybercrime”, zegt Hector Hamaker, verantwoordelijk voor Incident Response service binnen Aon. “Maar als er iets gebeurt, hoeft dat niet het einde van de wereld te zijn, mits je snel en adequaat reageert”.

Onderwijsinstellingen beheren grote hoeveelheden (gevoelige) gegevens, waaronder persoonlijke informatie van leerlingen, studenten en medewerkers. Dit maakt hen een aantrekkelijk doelwit voor cybercriminelen. Maar om slachtoffer te worden van cybercrime hoeft een school niet per se een specifiek doelwit te zijn. Cybercriminelen maken namelijk ook gebruik van zwaktes in software om op grote schaal cyberaanvallen in te zetten.

Lees verder >

Hoe groot is het cyberrisico binnen het onderwijs?

Daar kunnen onderwijsinstellingen net zo goed slachtoffer van worden, met vaak grote gevolgen. Net als bij een softwarefout of storing, zoals onlangs bij Crowdstrike, of indirect zoals in het geval van Iddink Learning Materials, waarbij persoonlijke informatie zoals namen, e-mailadressen en bankgegevens van klanten van Iddink Learning Materials, zijnde scholen en studenten die boeken of leermaterialen hebben besteld zijn geraakt.

Wat is de mogelijke impact van cybercrime op onderwijsinstellingen?

Onderwijsinstellingen hebben vaak een uitgebreide digitale infrastructuur. Dit geeft cybercriminelen steeds meer mogelijkheden om toe te slaan met bijvoorbeeld ransomware, phishingmails of ongeautoriseerde toegang tot systemen. Die dreiging kan overigens ook van binnenuit komen, bijvoorbeeld van medewerkers of studenten. De gevolgen zijn vaak zeer omvangrijk. Denk daarbij aan:

- Verstoring van het onderwijs, examinering en administratieve processen
- Financiële schade door afpersing of herstelkosten
- Reputatieschade en verlies van vertrouwen bij ouders en studenten
- Datalekken en verlies van persoonlijke gegevens met mogelijke juridische consequenties
- Kosten van herstel en langdurige negatieve effecten op de digitale infrastructuur onderwijs cyberveiliger.

Welke verantwoordelijkheid hebben onderwijsinstellingen zelf?

“Er in ieder geval voor zorgen dat zij zo goed mogelijk beschermd zijn tegen cyberaanvallen. Maak een helder plan en neem de nodige preventieve (IT-) maatregelen aan de hand van het Normenkader Informatiebeveiliging en Privacy. Tegelijkertijd moeten we beseffen dat 100% cyberveiligheid niet bestaat. Het is daarom verstandig ook na te denken over het scenario waarin het toch fout gaat. Wie doet dan wat op zo’n moment? En welke hulplijnen kunt u inschakelen? Schiet je in de paniek en maak je de verkeerde keuzes, dan kunnen de gevolgen veel ernstiger zijn dan nodig. Bestuurders hebben hierbij de verantwoordelijk voor alle belanghebbenden om proactief te handelen. Het Normenkader helpt daarbij, maar het is belangrijk ook zelf daadkracht te tonen”.

Lees verder ›

Incident Response Service helpt

Hoe kunnen zij dat doen?
"Incident Response Service helpt onderwijsinstellingen snel en adequaat te reageren op cyberincidenten. Vooral in de eerste uren na een incident biedt het veel toegevoegde waarde.

Via een speciaal telefoonnummer kunnen onderwijsinstellingen 24/7 bij Aon terecht. We helpen hen met antwoord op hulpvragen en brengen ze in contact met de juiste partijen. Als een spin in het web begeleiden wij het hele proces.

Door direct vanaf het eerste moment op de juiste manier te handelen, kan veel schade voorkomen en beperkt worden."

Wat houdt Incident Response Service precies in?
Voor een vast maandelijks bedrag van 100 euro (exclusief btw) krijgt u de volgende service:

- 24/7 toegang tot het incident response-team via het speciale noodnummer
- Toegang tot ons netwerk van geverifieerde specialisten tegen gereduceerde tarieven
- Een consult met een cyberspecialist
- 8 uur-incidentbegeleiding door een ervaren incident response-consultant
- Een sjabloon van een standaard crisiskaart voor incidenten
- Uitnodiging voor een halfjaarlijkse kennissessie met ervaringen uit de praktijk (webinar)
- Korting op onze cybersimulatie-oefeningen

Let op, dit abonnement heeft een looptijd van een jaar en is daarna maandelijks opzegbaar.

Vragen?
Wilt u meer weten over cyberveiligheid binnen het onderwijs? Bel dan met ons Incident Response-team. Of meld u aan voor het webinar Incident Response in het onderwijs op donderdag 3 oktober. Dan nemen we alle informatie van a tot z door.

Download hier onze folder over Incident Response

Generatieve AI in het onderwijs: Kans of risico?

Generatieve AI verandert het onderwijslandschap snel en ingrijpend en biedt veelbelovende kansen voor het verbeteren van onderwijsprocessen en leerervaringen. Deze nieuwe technologie gebruikt machine learning om content te creëren, zoals tekst, beelden en geluid. Naast kansen brengt Generatieve AI ook aanzienlijke risico's met zich mee voor het onderwijs die zorgvuldig moeten worden beheerd.

In een recent sectorbeeld benadrukt de Autoriteit Persoonsgegevens de urgente maatschappelijke en privacy-uitdagingen voor de onderwijssector en dat algoritmes en AI vragen om nieuw beleid en een gesprek over hun wenselijkheid.

We hebben belangrijke kansen en risico's kort onder elkaar gezet.

Lees verder >

Kansen van Generatieve AI:

1. **Persoonlijke Leerervaringen:** AI kan op maat gemaakte leermaterialen creëren die inspelen op de individuele behoeften van leerlingen/studenten, wat de effectiviteit van het leren verhoogt

2. **Ondersteuning voor Docenten:** AI kan routinetaken automatiseren, zoals het opstellen van toetsen en nakijken van werkstukken, waardoor docenten meer tijd overhouden voor interactie met leerlingen.

3. **Creatieve en Interactieve Leermethoden:** AI-gebaseerde simulaties en lessen maken complexe concepten toegankelijker en boeiender.

Risico's van Generatieve AI:

1. **Kwaliteit en Betrouwbaarheid:** AI kan fouten maken of ongepaste inhoud genereren, wat kan leiden tot misinformatie.

2. **Privacy en Beveiliging:** Het gebruik van AI vereist vaak grote hoeveelheden data, wat risico's met zich meebrengt voor de privacy en beveiliging van informatie.

3. **Ethische Overwegingen:** AI kan biases versterken, wat kan leiden tot ongelijke behandeling van leerlingen/studenten.

4. **Fraude en Cyberincidenten:** AI kan worden misbruikt voor fraude, zoals het vervalsen van opdrachten, en kan zelf doelwit worden van cyberaanvallen.

Mitigeer de risico's:

1. **Strikt toezicht en regels:** Onderwijsinstellingen moeten duidelijke richtlijnen opstellen voor het gebruik van generatieve AI, inclusief ethische normen en privacybeleid.

2. **Training en bewustwording:** Docenten en leerlingen/studenten moeten worden getraind in het verantwoord gebruik van AI-technologieën en worden geïnformeerd over de potentiële risico's..

3. **Technologische veiligheidsmaatregelen:** Implementatie van cybersecurityprotocollen om de data en systemen te beschermen tegen aanvallen en misbruik.

Aanbevelingen

Generatieve AI biedt kansen voor het onderwijs, echter niet zonder aandacht voor risicobeheer.

1. **Risicobeoordeling en -beheer:** Voer regelmatig risicobeoordelingen uit om potentiële bedreigingen te identificeren en te beheren.

2. **Continueringsplanning:** Ontwikkel een continuïteitsplan om snel te kunnen reageren op incidenten en de impact op uw organisatie te minimaliseren.

3. **Verzekering:** Overweeg een cyber- en fraude-verzekering om financiële risico's af te dekken.

> "Bestuurders, beslissers en adviseurs in het onderwijs moeten deze risico's begrijpen, grip krijgen en actie ondernemen op de onduidelijkheden."

Aanvullende informatie

We hebben een samenvattend document over de kansen en risico's van AI in het onderwijs opgesteld. **Download hier** het document 'AI in het onderwijs'.

Wilt u risicoadvies over AI?

Neem vandaag nog contact op met Aon om te bespreken hoe wij uw organisatie kunnen helpen bij het risicobeheer van AI. Samen maken we het gebruik van AI binnen het onderwijs veiliger.

Cyberbeveiliging gaat pas echt leven als de bestuurder overtuigd is

NUOVO Scholen, de stichting voor openbaar voortgezet onderwijs in Utrecht en omgeving, besloot enkele jaren geleden tot het afsluiten van een cyberverzekering. Hoe kwamen ze tot deze keuze en welke stappen gingen daaraan vooraf? “Als cyber alleen een onderwerp van IT is, blijft het een ‘papieren tijger’. Pas met commitment uit de Raad van Toezicht, hebben we cyberbeveiliging kunnen omzetten naar beleid dat echt leeft binnen onze organisatie”. Lees nu het verhaal van NUOVO.

Wat was de aanleiding om cyberbeveiliging naar een hoger plan te tillen?
Cyro van Malsen, manager onderwijsapplicaties bij NUOVO: “Aan de ene kant lazen wij in de krant over de cyberincidenten bij andere scholen. Tegelijkertijd kregen we ook te maken met het Normenkader Informatiebeveiliging en Privacy voor het onderwijs waar we aan moeten voldoen. Wij hebben daar zelf ook aan meegewerkt in verschillende werkgroepen, dus wisten al vroeg wat er van ons verwacht zou worden”.

Was dit voldoende om de organisatie te overtuigen van een cyberverzekering?
“Nee”, reageert Gert van Milligen, (extern) strategisch adviseur, “het heeft erg geholpen dat de Raad van Toezicht zich in dezelfde tijd meer zorgen begon te maken over de mogelijke gevolgen van een cyberincident. Voorop gesteld willen als NUOVO een veilige school zijn, ook ten aanzien van digitale veiligheid. Bestuurders zijn eindverantwoordelijk voor cyberveiligheid en kunnen aansprakelijk gesteld worden als hen onverantwoordelijk bestuur kan worden verweten. Dus zij wilden ook graag weten of we goed verzekerd waren in het geval er iets mis zou gaan. Als cyberbeveiliging puur als een IT-aangelegenheid wordt gezien, is het vaak lastig om er meer investeringen voor los te krijgen. Het belang en de urgentie ervan moeten echt van bovenaf erkend worden”.

nuovo scholen

Lees verder >

Hoe hebben jullie ervoor gezorgd dat cyberbeveiliging echt gaat leven?

Cyro: “Wij hebben onze cyberbeveiliging aangepakt op het gebied van techniek, procedures en organisatie. Dit is wat ons betreft essentieel. Als alleen de IT-afdeling zich ermee bezig houdt, gaat het niet werken. De hele organisatie - bestuur, medewerkers en leerlingen - speelt een rol bij cyberveiligheid. En ook onze leveranciers houden wij aan onze normen. Wij stellen bijvoorbeeld de voorwaarde dat zij ook ‘table top’-oefeningen* doen. Je kunt zelf alles op orde hebben, maar als het verderop in de keten fout gaat, ben je nog steeds net zo kwetsbaar. Dat heeft dus gevolgen gehad voor onze Europese aanbestedingen van onder meer de werkplekbeheerder en leveranciers van printers en telefonie.”

En hoe past een cyberverzekering in dit verhaal?
Gert: “Uiteraard hebben wij ons afgevraagd of we een cyberverzekering nodig hebben. Je betaalt toch premie, maar het kan niet voorkomen dat je slachtoffer wordt. Wat heb je er dan precies aan? Het grappige is, dat het een beetje andersom werkt. Om aanspraak te kunnen maken op de dekking van een cyberverzekering moet je aan voorwaarden voldoen. Maar door dat te doen, word je een cyberveilige organisatie. Het dwingt ons om te blijven voldoen aan de eisen en up-to-date te blijven. En als er dan toch een cyberincident plaatsvindt, zijn veel kosten die je maakt gedekt. Daarnaast krijg je vanuit de verzekeraar allerlei ondersteuning om de schade zo veel mogelijk te beperken en snel weer up-and-running te zijn. Dat gaat verder dan alleen het herstellen van de systemen, maar bijvoorbeeld ook om imagoschade te voorkomen.”

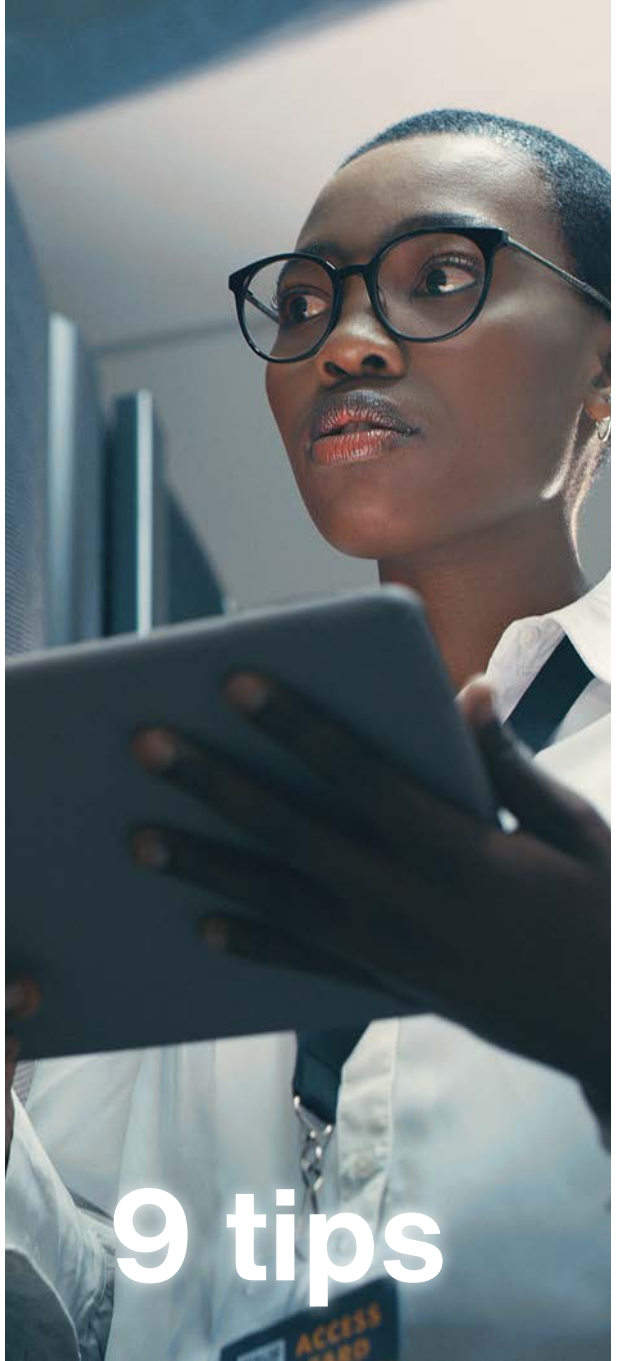
Welke tip zouden jullie willen geven aan collega-bestuurders en beslissers in het onderwijs?
“Neem beveiliging echt serieus”, reageert Gert. “Ik denk dat veel scholen zich afvragen hoe interessant zij zijn voor cybercriminelen, maar je hoeft tegenwoordig geen doelwit te zijn om slachtoffer te worden. Als er ergens een deur open staat, komen ze binnen. En pas dan kijken de criminelen hoe ze er een slaatje uit kunnen slaan. Maar dan is voor de school het leed al geleden”.

Cyro vult aan: “Besef daarbij dat het niet alleen om de techniek gaat. Je kunt een mooi slot op de deur hebben, maar als je de sleutel in het slot laat zitten dan heeft het geen toegevoegde waarde. Het gaat dus om de hele organisatie en de procedures die je met elkaar afspreekt. Wij hebben veiligheid hoog in het vaandel staan en vanuit de maatschappij wordt dat ook verwacht van het onderwijs. Niet alleen in het gebouw en op het schoolplein, maar ook in de digitale wereld.”

*Table top Nuovo gaat met de leveranciers in de keten testen om te controleren of de cyberweerbaarheid op orde is en/of waar deze kan worden verbeterd.

Het Aon Cybersecurity team
De rol van het Aon Cybersecurity team omvat het jaarlijks benchmarken van de cyberverzekering. Hierbij wordt in duidelijke en overzichtelijke taal uitleg gegeven over trends, ontwikkelingen, schadecijfers, typen cyberschade en de verzekerde bedragen. Dit stelt het bestuur in staat om een weloverwogen beslissing te nemen over de adequaatheid van de huidige verzekeringsoplossing.

Meer weten over CyberHulp voor uw organisatie?
Neem contact met ons op om te leren hoe wij kunnen helpen uw cyberweerbaarheid te verbeteren.



Nieuw onderwijsjaar, nieuwe medewerkers en leerlingen /studenten?

9 Tips om de Cyber-weerbaarheid te Verhogen

In een steeds digitaler wordende wereld zijn onderwijsinstellingen kwetsbaarder dan ooit voor cyberdreigingen. Met de toename van online onderwijs en digitale leeromgevingen is het essentieel dat nieuwe medewerkers, leerlingen en studenten goed zijn voorbereid om deze dreigingen te herkennen en af te weren. Hier zijn 9 tips om de cyberweerbaarheid te vergroten.

1 **Bewustwording en training**
Zorg ervoor dat zowel medewerkers als leerlingen/studenten zich bewust zijn van cyberrisico's zoals phishing en ransomware. Gerichte introductietrainingen en regelmatige herhalingstrainingen houden deze kennis actueel.

2 **Cyberveiligheid in het curriculum**
Integreer cyberveiligheid in het onderwijs-programma. Van basislessen over veilige wachtwoorden tot geavanceerde onderwerpen zoals informatiebeveiliging voor oudere studenten. Ook medewerkers kunnen profiteren van continue educatie en certificering.

3 **Beveiligingstechnologieën implementeren:**
Investeer in geavanceerde technologieën zoals multi-factor authenticatie en Managed Detection & Response (MDR) om ongeautoriseerde toegang te voorkomen en data te beschermen.

4 **Sterk beleid en protocol**
Stel duidelijke beleidslijnen en protocollen op voor wachtwoordbeheer en gegevens-bescherming. Regelmatige simulaties kunnen helpen bij de voorbereiding op een daadwerkelijke cybercrisis.

5 **Veilig gebruik van apparaten en netwerken**
Moedig het veilige gebruik van apparaten en netwerken aan. Overweeg richtlijnen zoals het verbod op smartphones tijdens de les, die vanaf het schooljaar 2024-2025 worden uitgebreid naar het basisonderwijs.

Lees verder >

6 **Betrekken van ouders en verzorgers**
Informeer ouders over de gevaren van het internet en hoe ze hun kinderen kunnen ondersteunen bij het herkennen van dreigingen. Dit kan via ouderavonden en nieuwsbrieven.

7 **Incident Response en beleid**
Zorg voor een duidelijk beleid voor Incident Response. Iedereen binnen de instelling moet weten wat te doen bij een cyberincident om schade te minimaliseren.

8 **Samenwerken met Experts**
Onderwijsinstellingen kunnen profiteren van samenwerking met cybersecurity-experts voor advies en ondersteuning. Dit verhoogt de weerbaarheid tegen cyberdreigingen.

9 **Continue evaluatie en verbetering**
Voer regelmatig audits uit en beoordeel de huidige beveiligingsmaatregelen. Zo blijft de instelling op de hoogte van de snel veranderende aard van cyberdreigingen.

9 tips

Cyberveiligheid is voortdurende inspanning
Met deze geïntegreerde aanpak kunnen onderwijsinstellingen hun medewerkers en leerlingen/studenten effectief beschermen tegen cyberdreigingen. Cyberveiligheid vraagt om constante aandacht en proactieve maatregelen in een steeds veranderende technologische wereld.

Meer weten?
Neem contact met ons op om te leren hoe wij kunnen helpen uw cyberweerbaarheid te verbeteren.

Is uw onderwijsinstelling voorbereid op een calamiteit of crisis?

Onderwijsinstellingen kunnen te maken krijgen met verschillende soorten crises, zoals studentenprotesten, schietincidenten, en cyberaanvallen. Bestuurders zijn verantwoordelijk voor de veiligheid van leerlingen, studenten, medewerkers en ouders, en moeten daarom goed voorbereid zijn op crisissituaties. Crises en calamiteiten kunnen fysiek, financieel, technisch, cybergerelateerd als sociaal van aard zijn. De gevolgen zijn daarom ook zeer uiteenlopend.

Verschillen in risicoprofiel

Iedere onderwijsinstelling heeft een ander risicoprofiel; alle risico's verschillen in soort en omvang. Zo is een universiteit een open en internationaal instituut, waar mensen in- en uit kunnen lopen en de afhankelijkheid van data groter is dan in het primair onderwijs. (Cyber)risico's kunnen hier zelfs staatsgedreven zijn. Bij middelbare scholen en ROC's ligt de nadruk meer op fysiek geweld en sociale veiligheid. Met als trieste dieptepunten het tram incident in Utrecht vlakbij school en het doodgeschoten meisje van 16 in de fietsenstalling van de school in Rotterdam. Omdat daar ook minderjarige leerlingen/studenten onderwijs volgen, hebben onderwijsinstellingen ook te maken met hun zorgplicht. Maar hoe ver gaat dat? In figuurlijke zin, tegenover ouders en andere belanghebbenden, maar ook in letterlijke zin; tot hoe ver buiten de schoollocatie gaat uw verantwoordelijkheid?

Lees verder ›

“Hoe heeft u uw verantwoordelijkheden belegt en hoe bereidt u zich het beste voor?”

Aan het woord zijn Menno Jansen en Daniëlle Ohler van het Instituut voor Veiligheid en Crisismanagement (COT). Menno “Iedere onderwijsinstelling heeft een ander risicoprofiel en risico’s verschillen in soort en omvang. Zo is een universiteit een open en internationaal instituut, waar mensen in- en uit kunnen lopen en de afhankelijkheid van data groter is dan in het primair onderwijs. (Cyber)risico’s kunnen hier zelfs staatsgedreven zijn. Bij middelbare scholen en mbo’s ligt de nadruk meer op fysiek geweld en sociale veiligheid. Voorbeelden van calamiteiten met grote impact op leerlingen/onderwijsinstellingen zijn het tramincident in Utrecht, en een dodelijke steekpartij in Rotterdam op een school”. Laat staan de aantallen keren dat er een dodelijk ongeluk is van een kind onderweg van of naar school.”

Daniëlle vult aan “Omdat daar ook minderjarige leerlingen/studenten onderwijs volgen, hebben onderwijsinstellingen ook te maken met hun zorgplicht. Maar hoe ver gaat dat? In figuurlijke zin, tegenover ouders en andere belanghebbenden, maar ook in letterlijke zin; tot hoe ver buiten de schoollocatie gaat uw verantwoordelijkheid?”

Reactie en communicatie vanuit bestuur

Danielle “Veiligheidsplannen zijn bij de meeste onderwijsinstellingen goed op orde, maar (vooral in het basis- en voortgezet onderwijs) zijn directies regelmatig onvoldoende voorbereid op een crisis. Het is belangrijk om vooraf goed na te denken over hoe u als bestuurder omgaat met een crisis op het moment dat deze zich voordoet. Welke risico’s spelen er in welke scenario’s? En hoe reageert u daarop? Sluit u zich simpelweg aan bij de communicatie vanuit de koepel? Of formuleert u een eigen perspectief op basis van uw beleid en visie?”

Verantwoordelijkheid van bestuurders

Menno “Als er een calamiteit plaatsvindt, komen er op bestuurders van onderwijsinstellingen direct veel vragen af: Wie is er getroffen? Wie heeft er ‘pijn’? En wie kan ons helpen? Er wordt van u als bestuurder verwacht dat u snel en adequaat reageert.
Dit vereist dat u:

- snapt hoe u moet omgaan met de media;
- helder communiceert en afspraken maakt met interne en externe partners (zoals de politie);
- hulp inroept van ervaringsdeskundigen, zoals mensen met crisisvaardigheden binnen de koepel.”

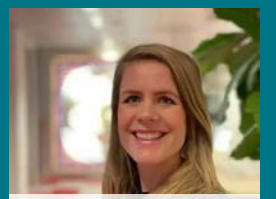
Succesvol managen van een crisis Voor het succesvol managen van een crisis is het van belang dat bestuurders beschikken over crisisvaardigheden en weten wanneer ze hulp moeten inroepen. Aon en het COT bieden ondersteuning en trainingen aan schoolbesturen om hen te helpen beter voorbereid te zijn op verschillende scenario’s. Deze trainingen richten zich op het oefenen en evalueren van vaardigheden en dilemma’s.

“Er wordt van u als bestuurder verwacht, dat u snel en adequaat reageert.”

Markeer alvast maart 2025 in uw agenda!
Dan organiseert SURF de twee jaarlijkse OZON-oefening, waarin MBO- en HBO instellingen en Universiteiten weer kunnen deelnemen aan een grootschalige Cybercrisis oefening. Het COT is bij deze oefening ook betrokken, in ons komend onderWIJS magazine leest u hier meer over. Zo blijft u voorbereid op mogelijke crisissen.

Bezoek ook de website van het COT

Menno Jansen



Daniëlle Ohler

Wij beantwoorden uw vragen graag

Wij brengen uw risico's in kaart en helpen u met advies op het gebied van risicomanagement, duurzame inzetbaarheid en vitaliteit, crisis- en calamiteitenmanagement en passende verzekeringsoplossingen voor u en uw organisatie.

Heeft u naar aanleiding van een van de artikelen vragen of wilt u een vrijblijvend adviesgesprek met een van onze adviseurs?

Voor PO en VO neem contact op met:
Henri Damen
06 13817417
henri.damen@aon.nl

Voor MBO, HBO of Universiteiten neem contact op met:
Harm Mulder
06 49332328
harm.mulder@aon.nl

De voordelen van Aon

- Meer dan 50 jaar ervaring met advisering en schade-afhandeling in het onderwijs
- Wij gidsen onderwijsbesturen door de complexe verzekeringswereld
- We adviseren u persoonlijk om de juiste beslissingen te nemen met een vaste adviseur
- Goede en snelle begeleiding bij schade door een vaste contactpersoon