School CERT door Kennisnet in samenwerking met SIVON

Dreigingsbeeld Cybersecurity primair en voortgezet onderwijs 2025

Kwetsbaarheden herkennen, veiligheid verhogen

Laat ICT werken **voor het onderwijs**

Inhoudsopgave

Voorwoord

Voor je ligt het Dreigingsbeeld Cybersecurity voor het primair en voortgezet onderwijs, dat scholen ondersteunt bij het identificeren van de dreigingen waartegen zij zich moeten beschermen. Dit dreigingsbeeld helpt jouw schoolbestuur zich voor te bereiden op deze dreigingen en verduidelijkt wat ze concreet inhouden. Daarnaast bevat elke dreiging een praktijkverhaal van mensen die in hun werk te maken hebben met deze dreigingen.

De dreigingen die we in dit dreigingsbeeld belichten, zijn niet de enige waarmee de sector te maken heeft, maar volgens School-CERT wel de belangrijkste. Er zijn ook indirecte dreigingen die de kans vergroten dat een schoolbestuur wordt getroffen of die de impact van een incident verergeren. Bijvoorbeeld bij een gebrek aan capaciteit, middelen en kennis bij schoolbesturen, waardoor een organisatie onvoldoende is voorbereid op een cybersecurity-incident.

We hopen dat dit dreigingsbeeld schoolbesturen helpt zich beter voor te bereiden op de dreigingen die op hen afkomen. Op die manier kunnen we met elkaar het onderwijs digitaal veilig houden.

(Management)samenvatting

Het onderwijs is net als veel andere sectoren steeds afhankelijker van ICT. Naast digitale administratie-systemen worden ook andere digitale middelen steeds vaker gebruikt. Een veilige en robuuste digitale school-omgeving is belangrijk voor alle betrokkenen.

School-CERT ziet sinds het vorige dreigingsbeeld, uit 2023, een stijging van het aantal digitale aanvallen in het primair en voortgezet onderwijs. Kwaadwillenden kunnen tegenwoordig, door technologische vooruitgang, eenvoudiger een aanval uitvoeren. De aanvallen zijn moeilijker te herkennen. En er worden veel malafide diensten aangeboden die de kwaadwillenden helpen om een aanval uit te voeren. Het is daarom niet langer de vraag óf er een aanval op een school(bestuur) zal plaatsvinden, maar wanneer. Door deze toename staat de digitale veiligheid op scholen onder druk en daarmee ook de continuïteit van het onderwijs. Middelen en kennis om de dreigingen het hoofd te bieden, zijn helaas vaak beperkt beschikbaar in het onderwijs.

De voornaamste cyberdreigingen zijn:

- **DDoS**: uitval van ICT-systemen door bewuste overbelasting waardoor onderwijsprocessen gevaar lopen.
- **Afhankelijkheid van leveranciers**: ICT-incidenten bij leveranciers waardoor de veilige en beschikbare onderwijsomgeving gevaar loopt.
- **Infostealers**: het stelen van gegevens door middel van schadelijke software. Deze gegevens kunnen vervolgens voor fraude of afpersing worden gebruikt.
- **Phishing**: het bemachtigen van persoonlijke (toegangs)- gegevens door social engineering (misleiding en manipulatie), waarna fraude, oplichting of afpersing kan plaatsvinden.
- **Ransomware**: het gijzelen van (gevoelige) data en systemen door criminelen. Hierbij wordt scholen verteld dat, als ze niet aan de eisen voldoen, de lokale data wordt vernietigd en/of gepubliceerd op het darkweb (chantage).

Deze dreigingen en aanvallen hebben als voornaamste gevolg dat middelen en diensten minder goed of helemaal niet meer beschikbaar zijn voor gebruikers. Dit wordt veroorzaakt door:

- (Identiteits)diefstal, fraude, oplichting.
- Afpersing en sabotage.
- Tekorten aan ICT-securitykennis en nalevingscontrole.

In 2025 vonden in Nederland meerdere digitale aanvallen plaats die impact hadden op schoolprocessen en bedrijfsvoering. De gevolgen die School-CERT heeft gezien zijn:

- Verstoring van het onderwijs door ransomwareaanvallen.
- Leveringsvertraging van bestellingen en uitgevallen school-examens door cyberincidenten bij leveranciers.
- Frauduleuze bestellingen uit naam van schoolbesturen.
- Misbruik van ICT-middelen waardoor systemen onderdeel worden van botnets. Een botnet is een netwerk van computers of apparaten die ongemerkt door kwaadwillenden zijn overgenomen en op afstand worden aangestuurd.
- Afhandig maken van inloggegevens.

Doordat een aanval eenvoudig en tegen lage kosten als product kan worden afgenomen, worden zowel de continuïteit van het onderwijs als het imago van scholen bedreigd. Verbetering van de samenwerking binnen het onderwijs is noodzakelijk, om de weerbaarheid tegen deze dreigingen en aanvallen te vergroten.

Door risicoanalyses uit te (laten) voeren op basis van dit dreigingsbeeld, kun je vaststellen welke dreigingen het meest relevant zijn voor jouw schoolbestuur. In het Normenkader IBP vind je normen en maatregelen die je kunt toepassen. Om hier praktisch mee aan de slag te gaan, biedt het Groeipad een aantal deelprojecten die je kunt gebruiken. Bijvoorbeeld voor het beheersen van risico's, het goed afhandelen van incidenten en datalekken en het waarborgen van bedrijfscontinuïteit. Bij elk deelproject vind je heldere toelichting, een handig stappenplan en praktische voorbeelddocumenten.

Dreigingen

In het dreigingsbeeld lichten we de meest relevante dreigingen toe. Bij elke dreiging die we bespreken, geven we een praktijkvoorbeeld en handvatten die helpen je weerbaarheid tegen deze dreiging te vergroten.

De dreigingen zijn gekozen op basis van observaties van School-CERT. Om de relevantie van dreigingen te bepalen, hebben we drie criteria gebruikt:

1. Hoe groot is de kans om slachtoffer te worden?
2. Wat is de impact op de continuïteit van het onderwijs?
3. Wat is de impact op de veiligheid van data?

Na het toetsen op deze criteria door School-CERT, zijn er vijf belangrijke dreigingen uitgewerkt. Deze dreigingen vormen momenteel de grootste risico's voor het primair en voorgezet onderwijs.

Hoewel Artificial Intelligence (AI) de afgelopen twee jaar een ontwikkeling heeft doorgemaakt die aandacht vereist, hebben we dit bewust niet als dreiging opgenomen. We zien AI namelijk niet als een dreiging op zich, maar als een katalysator voor andere dreigingen. AI maakt het makkelijker en goedkoper om sneller kwaadaardige software, kwaadaardige scripts of phishing te ontwikkelen en slachtoffers te maken. Het kan op basis van een simpele instructie - een prompt - werkende malware (kwaadaardige software) ontwikkelen waardoor de drempel voor cybercriminelen lager is; ze hoeven geen technische vaardigheden te hebben. Tegelijkertijd kan AI ook worden ingezet om de beveiliging tegen hackers te verbeteren, aangezien het steeds vaker wordt geïntegreerd in veiligheidsproducten zoals firewalls en online omgevingen.

Kortom: gezien de huidige rol in het cyberlandschap beschouwen wij AI op dit moment nog niet als concrete dreiging. We zijn ons wel bewust van de mogelijke risico's, maar zien er ook een middel in om de cyberveiligheid juist te verhogen.

Inzicht in digitale kwetsbaarheden

Digitale leeromgevingen, toetsplatforms en leerlingadministratie spelen dagelijks een rol in het functioneren van scholen. Het Nederlandse onderwijs draait grotendeels op ICT. Dat is ook logisch: digitale middelen maken het onderwijs efficiënter, toegankelijker en beter aanpasbaar op de behoeften van leerlingen en leraren. Gevolg is wel dat scholen erg afhankelijk zijn van ICT, wat betekent dat de consequenties groot kunnen zijn wanneer er iets misgaat. Bijvoorbeeld als systemen plotseling niet beschikbaar zijn of als gevoelige informatie in verkeerde handen valt. Het doel is dat te voorkomen.

Beperkte capaciteit en kennis

Scholen hebben te maken met een kwetsbare doelgroep: kinderen. Ze verwerken namen, adressen, medische gegevens en toetsresultaten. Omdat het om minderjarigen gaat, is het extra belangrijk dat deze gegevens goed worden beschermd. De Autoriteit Persoonsgegevens benadrukt dat kinderen in het onderwijs recht hebben op extra bescherming, zodat ze zich vrij en veilig kunnen ontwikkelen.[1] Goede digitale veiligheid is daarbij een voorwaarde.

In de praktijk beschikken scholen echter niet altijd over voldoende middelen, tijd of expertise om adequaat in te spelen op digitale dreigingen en nieuwe technologieën. Een nulmeting op basis van het Normenkader Informatiebeveiliging en Privacy (IBP) toonde in 2023 aan dat geen van de onderzochte schoolbesturen op dat moment volledig voldeed aan het gewenste niveau op de voorgestelde normen.[2] Dit betekent niet dat scholen niets doen, maar dat er wel verbeteringen nodig zijn om hun digitale weerbaarheid te versterken.

Scholen als (on)bedoeld doelwit

Een hardnekkig misverstand is dat scholen geen interessante doelwitten zijn voor cybercriminelen. In werkelijkheid zijn ze juist zeer interessant, omdat ze over gevoelige persoonsgegevens van leerlingen, medewerkers en ouders beschikken. Hoewel cybercriminelen meestal grotere organisaties aanvallen, worden scholen ook vaak indirect getroffen. Bijvoorbeeld doordat criminelen steeds vaker gebruikmaken van geautomatiseerde of gestandaardiseerde aanvalsmethoden of zich richten op leveranciers. Daarnaast zijn er risico's van binnenuit, zoals leerlingen die proberen toegang te krijgen tot systemen zonder zich bewust te zijn van de mogelijke gevolgen.

Houvast door inzicht

Dit dreigingsbeeld biedt schoolbesturen inzicht in de belangrijkste digitale dreigingen voor het primair en voortgezet onderwijs die door School-CERT zijn gesignaleerd. Het laat zien welke risico's van belang zijn, waar er mogelijk kwetsbaarheden liggen en wat je kunt doen om deze risico's te verkleinen. Door als schoolorganisatie bewuster met cyberveiligheid om te gaan, werk je aan de digitale weerbaarheid van het onderwijs en daarmee aan een veilige leeromgeving voor alle leerlingen in Nederland.

1 *Trends, risico's en aanbevelingen over de bescherming van persoonsgegevens bij digitalisering in het onderwijs, 2021, Autoriteit Persoonsgegevens*

2 *Nulmeting Normenkader IBP: waar staat het funderend onderwijs met informatiebeveiliging?, Kennisnet*

DDoS

DDoS staat voor Distributed Denial of Service. Bij een DDoS-aanval stuurt iemand in korte tijd zoveel mogelijk data naar een systeem, waardoor dat onbereikbaar wordt voor het overige verkeer. Een DDoS-aanval is een relevante dreiging voor het onderwijs, omdat de aanval eenvoudig uit te voeren is.

Bij zo'n aanval kunnen het netwerk of de online diensten van een school verstoord raken. Dat heeft niet alleen impact op de apparatuur, maar kan ook tot grote verstoring van het onderwijs leiden, zoals niet online kunnen werken of niet kunnen afnemen van digitale toetsen.

Een DDoS-aanval is een laagdrempelige aanvalsmethode, omdat het gemakkelijk uit te voeren is en de kosten voor de aanvaller laag zijn. Er zijn veel websites die voor weinig geld (of zelfs gratis) een DDoS-aanval uitvoeren op het systeem dat de aanvaller wil verstoren. De aanvallers zijn in veel gevallen dan ook geen professionele hackers, maar leerlingen van de onderwijsinstelling zelf, die op deze manier laagdrempelig een aanval kunnen uitvoeren. Bijvoorbeeld omdat ze bewust het onderwijs of een toets willen verstoren, of omdat ze iets willen uitproberen zonder dat ze de consequenties ervan overzien.

Uit de praktijk

Om een beeld te krijgen van de impact van DDoS-aanvallen sprak School-CERT met een ICT-coördinator uit het noorden van het land. Dit is zijn ervaring van de DDoS-aanval op SURF, van begin 2025.

De eerste dag begon met een melding dat de printers niet werkten. Dit was geen ongewone melding, dus het leidde niet direct tot een alarm. Wel werd er een onderzoek gestart naar deze melding en al snel kwamen er meldingen dat ook Magister niet werkte. Hierdoor groeide het besef dat het wel eens flink mis kon zijn.

We merkten al snel dat de problemen gerelateerd waren aan het netwerk. De WiFi werkte wel, maar we konden er niet mee verbinden en ook de rest van het netwerk had problemen. Naar aanleiding hiervan hebben wij direct een melding gemaakt bij ons hoofdkantoor en ons interne CERT-team. Onze stichting is een combinatie van voortgezet onderwijs en mbo. Deze locaties hadden allemaal problemen, dus we zagen al snel in dat de problemen wel bij de SURF-aansluiting moesten liggen.

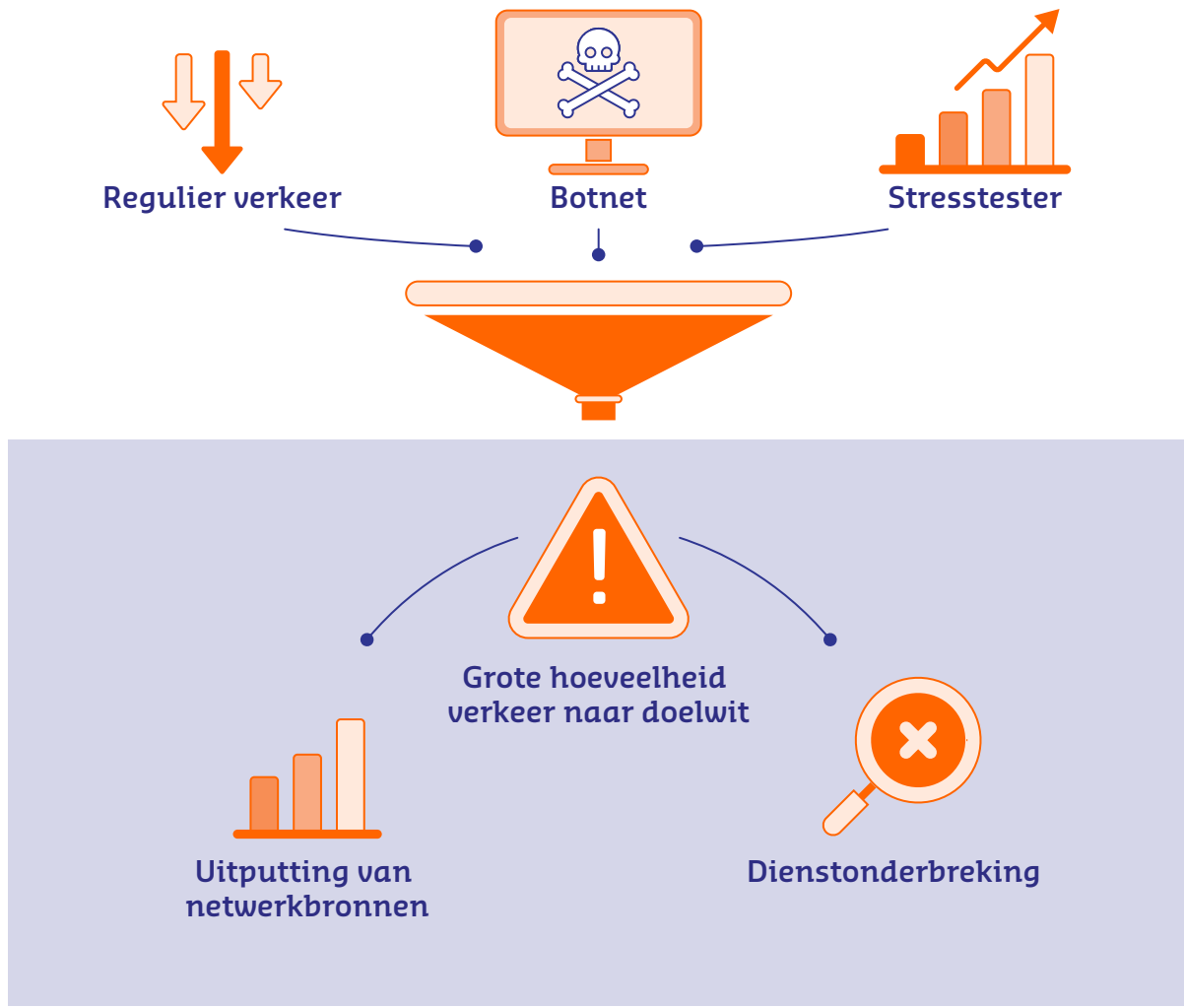
De mitigerende maatregelen die SURF nam, werkten onvoldoende. En de problemen leken zich ook uit te breiden. Aan het eind van de dag leek het opgelost, maar de volgende ochtend deden zich weer exact dezelfde problemen voor. Op de tweede dag waren er schoolexamens gepland die digitaal zouden plaatsvinden. We moesten toen beslissen of we de die zouden uitstellen.

We hebben ervoor gekozen dit te doen, omdat de doorgang van de examens niet gewaarborgd kon worden en het onduidelijk was hoe lang de problemen zouden aanhouden.

Na deze maatregel sprak het bestuur zijn zorgen uit over het verloop van de centrale examens, waarbij het netwerk ook een belangrijke rol speelt. De organisatie heeft na dit voorval de mogelijkheden onderzocht om een extra internetlijn aan te leggen, maar de voordelen daarvan bleken niet op te wegen tegen de kosten.

Het is lastig dat je zelf geen controle hebt. Je zorgt er als organisatie voor dat je cybersecurity goed op orde is, maar aanvallen als deze kun je niet voorkomen. Helaas hebben wij hier flink hinder van ondervonden en had het tot gevolg dat we examens moesten uitstellen.

DDoS-aanval


Regulier verkeer
Botnet
Stresstester
Grote hoeveelheid verkeer naar doelwit
Uitputting van netwerkbronnen
Dienstonderbreking

Wat ziet School-CERT?

DDoS-aanvallen blijven voor veel sectoren een probleem. Hoewel sinds het vierde kwartaal van 2024 het aantal DDoS-aanvallen afneemt, zien we dat de aanvallen grotere hoeveelheden data bevatten.[3] Daardoor zijn deze aanvallen moeilijker af te wenden en kunnen ze in potentie voor meer verstoring zorgen.

Aanvallen op andere sectoren kunnen ook invloed hebben op het onderwijs. Als een provider of een leverancier wordt getroffen door een DDoS-aanval, kunnen scholen daarvan ook de gevolgen merken. Dit werd ook duidelijk bij de DDoS-aanval op SURF begin 2025 die voor een grote verstoring in het onderwijs zorgde.

Uit statistieken van het NDC (Nationaal Dienstencentrum)[4] blijkt dat het grootste deel van de DDoS-aanvallen in het primair en voortgezet onderwijs plaatsvindt binnen het voortgezet onderwijs. Deze DDoS-aanvallen zijn over het algemeen klein en leveren weinig tot geen verstoring op voor de scholen. Dit wijst erop dat het waarschijnlijk om actoren gaat die een eerdergenoemde goedkope DDoS-dienst afnemen. De kans op verstoring door DDoS-aanvallen in het primair onderwijs is wel aanwezig, maar vooral omdat leveranciers getroffen kunnen worden door een aanval.

Hoe kan jouw bestuur zich voorbereiden op deze dreiging?

Helaas zijn er geen technische middelen beschikbaar om een DDoS-aanval te voorkomen. Wel kunnen er preventief technische maatregelen worden genomen om de impact van zo'n aanval te verkleinen. Zo zijn er firewalls waar DDoS-bescherming op in te schakelen is. Ook bieden zakelijke providers anti-DDoS services aan bij je internet- of hostingaansluiting. Verder is het belangrijk dat je al maatregelen hebt genomen voor het geval jouw schoolbestuur slachtoffer wordt van een DDoS-aanval. Denk aan het inrichten van een plan om met kortstondig netwerkverlies om te gaan of een plan om te zorgen dat je netwerkinfrastructuur up-to-date blijft.

Binnen het Groeipad van het Normenkader Informatiebeveiliging en Privacy kunnen de volgende deelprojecten helpen bij het voorbereiden van deze maatregelen:

- *Deelproject 2.4 – Omgaan met incidenten en datalekken*
- *Deelproject 2.7 – Beveiligingseisen en -maatregelen vastleggen in een beveiligingsbaseline*
- *Deelproject 2.9 – Managen van leveranciersrisico's*
- *Deelproject 2.10 – Waarborgen van bedrijfscontinuïteit*
- *Deelproject 3.1 – Onderhouden van de infrastructuur*

3 *Grotere en meer complexe DDoS aanvallen in eerste kwartaal 2025, NBIP*

4 *Nationaal Dienstencentrum, Kennisnet*

Incidenten in de media

De media berichtten recent van een aantal incidenten waarbij verschillende Nederlandse organisaties of instanties doelwit waren van DDoS-aanvallen. De motieven achter deze aanvallen zijn niet altijd bekend; ze kunnen een activistisch karakter hebben. Met name bij de recente DDoS-aanvallen op Nederlandse organisaties bleek dit het geval.[5] Tijdens deze aanvallen werden onder andere websites van gemeenten en steden getroffen. Deze aanvallen zijn geclaimd door een pro-Russische actor met een pro-Russisch ideologisch motief.

Ook DigiD had in de eerste helft van 2025 meerdere keren te maken met DDoS-aanvallen die grote impact hadden. Zo was het bijvoorbeeld niet mogelijk in te loggen bij DUO, het UWV of de patiëntomgeving van zorginstellingen.[6] Naar het motief van deze DDoS-aanvallen wordt momenteel onderzoek gedaan.

5 *Lopende DDoS-aanvallen op Nederlandse organisaties, NCSC*

6 *DigiD opnieuw tijdelijk onbereikbaar geweest door DDoS-aanval, NOS*

Afhankelijkheid van leveranciers

Het primair en voortgezet onderwijs heeft veel ICT- diensten uitbesteed. Een voorbeeld hiervan zijn Software-as-a-Service (SaaS)-oplossingen, waarbij een online (cloud) dienst wordt aangeschaft zonder dat eigen beheer nodig is. Dit heeft verschillende voordelen. Leveranciers hebben meer tijd en expertise om betrouwbare en veilige diensten te bieden. Daarnaast zijn er veel leveranciers die zich specifiek op het onderwijs richten en de sector goed begrijpen. Bovendien kan een leverancier technische diensten inkopen die voor een individuele school te duur zijn.

Het uitbesteden van ICT-diensten brengt echter ook risico's met zich mee. Het onderwijs is afhankelijk van een beperkt aantal leveranciers voor het functioneren van systemen en zelfs voor de continuïteit van het onderwijs. Als een van de leveranciers wordt getroffen door een cyberaanval, last heeft van een storing of failliet gaat, is de impact binnen de sector direct groot.

Daarnaast zijn scholen afhankelijk van de maatregelen die de leverancier heeft getroffen tegen cyberaanvallen. Zonder heldere afspraken hebben scholen maar beperkt inzicht in de informatiebeveiliging van de leveranciers. Die leveranciers beheren ook de gegevens van minderjarige leerlingen, terwijl de school eindverantwoordelijk blijft. Als een leverancier tekortschiet, zijn de gevolgen van een incident vooral voor de school. Tegelijkertijd heeft de school maar beperkt inzicht en middelen om de leverancier aan te zetten tot verbetering op dit vlak.

Uit de praktijk

Een ransomwareaanval op leermiddelendistributeur Iddink Learning Materials, waarbij grote hoeveelheden data werden gestolen en diverse systemen geïnfecteerd raakten.

In april 2024 werd leermiddelendistributeur Iddink Learning Materials getroffen door een ransomwareaanval. Tijdens deze aanval werden verschillende systemen geïnfecteerd en werden er grote hoeveelheden data gestolen. Zodra de aanval bekend was, nam Iddink contact op met SIVON voor hulp bij de communicatie richting ouders en leerlingen. SIVON nam deze taak op zich en benaderde ook snel School-CERT. Na onderzoek werd de omvang bekend van de gegevens die waren gestolen. Het betrof data die vele jaren teruggingen, zoals adres- en betaalgegevens die scholen aanleveren bij het bestellen van materialen voor het nieuwe schooljaar.

Er werd besloten om communicatie richting ouders en leerlingen op te stellen. Omdat het niet verstandig is een dergelijk datalek lang stil te houden, werd dit proactief aangepakt. School-CERT en SIVON zorgden voor verschillende communicatiemiddelen, waaronder berichten die scholen konden gebruiken om ouders en leerlingen te informeren, wekelijkse webinars waar scholen vragen konden stellen en doelgroepberichten [tegenwoordig Sector Alerts genoemd *red.*] om bekendheid te geven aan het incident.

Iddink Learning Materials heeft de aanvallers geen losgeld betaald, maar besloot zijn infrastructuur opnieuw op te bouwen. Dit kostte veel tijd in de toch al drukke bestelperiode voor het nieuwe schooljaar.

Bij de start van het schooljaar 2024-2025 waren er veel problemen met de uitlevering van leermaterialen aan scholen en leerlingen. Veel bestellingen werden niet op tijd of helemaal niet geleverd, waardoor leerlingen geen leermateriaal hadden. Hoewel niet met zekerheid is te zeggen dat dit direct te maken had met de ransomwareaanval van eerder dat kalenderjaar, heeft het zeker niet geholpen bij het verloop van de uitlevering.

Om dit probleem aan te pakken, besloot SIVON een taskforce op te richten om de leermiddelen zo snel mogelijk bij de scholen te krijgen. Ze deden dit in samenwerking met distributeurs en een grote onderwijsstichting, wat erin resulteerde dat de materialen binnen vier weken waren geleverd.

Dit voorval laat het risico zien van leveranciersafhankelijkheid in het onderwijs. Door een incident (of een opeenstapeling van incidenten) kan het gebeuren dat het schooljaar voor duizenden leerlingen niet start zoals het zou moeten, met alle gevolgen van dien.

Wat ziet School-CERT?

Afhankelijkheid van leveranciers komt voor in verschillende sectoren, niet alleen in het onderwijs. Wanneer veel bedrijven in een sector afhankelijk zijn van één of enkele leveranciers, wordt die sector kwetsbaar bij problemen. Dit geldt niet alleen bij een hack of ransomware, zoals bij Iddink Learning Materials, ook bij een storing die langer aanhoudt, leidt dit tot problemen. Dat zagen we bijvoorbeeld bij de storing bij Basispoort die voor problemen zorgde bij verschillende basisscholen.[7]

Het onderwijs kent een klein aantal leveranciers met een aanzienlijk marktaandeel. Wanneer één van deze leveranciers problemen ondervindt, raakt dat direct heel veel scholen. Alternatieven zijn vaak niet eenvoudig te realiseren; het zou voor een schoolbestuur duur en arbeidsintensief zijn om twee leerlingadministratiesystemen (LAS) naast elkaar te gebruiken voor het geval een systeem uitvalt.

School-CERT heeft de afgelopen twee jaar meerdere gevallen geregistreerd waarbij een aanval op een leverancier resulteerde in verstoringen op scholen. In sommige gevallen was de continuïteit van het onderwijs in gevaar waardoor leerlingen naar huis gestuurd moesten worden of schoolexamens niet konden doorgaan. Aangezien scholen verantwoordelijk zijn voor de gegevens van hun leerlingen, moeten zij bij dergelijke incidenten een datalek melden bij de Autoriteit Persoonsgegevens. De impact van dit soort incidenten is dan ook groot.

Daarnaast waren er de afgelopen twee jaar verschillende storingen bij leveranciers. Bij een langdurige verstoring is de impact op het onderwijs vergelijkbaar met die van een cyberaanval. Wanneer School-CERT ook storingen meeneemt in de analyse, blijkt dat de gevolgen van leveranciersafhankelijkheid op het primair en voortgezet onderwijs nog groter zijn.

Hoe kan jouw bestuur zich voorbereiden op deze dreiging?

School-CERT constateert dat scholen beperkte mogelijkheden hebben om zich te beschermen tegen deze dreiging. Scholen zijn afhankelijk van hun leveranciers, of ze tijdig updates doorvoeren en of ze hun de processen op orde hebben. Ze kunnen echter wel maatregelen nemen om snel te detecteren dat een probleem bij de leverancier ligt en hiervoor een plan van aanpak opstellen. Daarnaast is het maken van back-ups bij een andere partij dan de leverancier een effectieve manier om de afhankelijkheid te verminderen. De haalbaarheid van deze oplossing kan echter variëren, afhankelijk van de specifieke dienst of applicatie.

7 *Storingen bij afname digitale toetsen verholpen, PO-raad*

De belangrijkste manier om de regie te houden, is door goede afspraken te maken met leveranciers. Controleer ook of een leverancier zich houdt aan sectorafspraken, zoals het *privacyconvenant* en *Certificeringsschema informatiebeveiliging en privacy ROSA*.
Wil je aan de slag met leveranciersmanagement, bekijk dan dit deelproject uit het Groeipad bij het Normenkader IBP: *Deelproject 2.9 Managen van leveranciersrisico's - Normenkader informatiebeveiliging en privacy voor het onderwijs*

Doordat slecht een klein aantal leveranciers zich specifiek op het onderwijs richt, is het voor de sector ook mogelijk om zich te organiseren en invloed uit te oefenen. Een organisatie als SIVON kan hierbij helpen. Zo heeft SIVON in samenwerking met Kennisnet en SURF een Data Protection Impact Assesment (DPIA) laten uitvoeren op Google Workspace for Education, wat heeft geleid tot een verbeterde bescherming van de privacy van leerlingen.

Incidenten in de media

Een ransomware bij Iddink Learning Materials leidde tot problemen voor een groot aantal middelbare scholen.[8]

Een aanval op het netwerk van SURF waardoor het schoolnetwerk uitviel, zorgde op veel scholen voor internetproblemen.[9]

Niet alleen hacks, maar ook storingen kunnen een effect hebben op de sector. De storingen van Basispoort in januari 2024 zorgden bijvoorbeeld voor veel uitgestelde Cito-toetsen.[10]

De grote Amerikaanse IT-leverancier Powerschool levert voor ruim 60 miljoen leerlingen ICT en had te maken met een ransomwareaanval. Na betaling van het losgeld, gingen de hackers over op het afpersen van individuele scholen.[11]

8 *Gelderse schoolboekenleverancier Iddink getroffen door ransomware-aanval, Security.nl*
9 *DDoS-aanvallen op Surf veroorzaken lawine aan ict-storingen in onderwijs, Computable.nl*
10 *Storingen bij afname digitale toetsen verholpen, PO-Raad*
11 *PowerSchool hack: School boards face new ransom demands months after leak, Globalnews.ca*

Infostealers

Infostealers zijn een type malware (kwaadaardige software) dat is ontworpen om persoonlijke gegevens te stelen. Infostealers werken onopvallend en efficiënt waardoor ze vaak onopgemerkt blijven door gebruikers. Dit maakt infostealers een reële dreiging voor scholen: ze komen ongemerkt op apparaten terecht en blijven er ook actief.

Infostealers kunnen op je apparaat komen door het downloaden van niet-officiële software, via phishing-mails of via een nep-CAPTCHA. Als je op een schadelijke link klikt of verkeerde software downloadt kan de infostealer zonder dat je het merkt worden geactiveerd. Deze software kopieert vervolgens documenten, wachtwoorden, adressen, browsergeschiedenis, cookies en gegevens van sociale media naar de computer van de aanvaller. De gestolen informatie wordt door criminelen gebruikt voor verschillende doeleinden, zoals verkoop op het dark web, toegang tot je sociale media of het plegen van identiteitsfraude.

Uit de praktijk

Het inlichten van scholen na de vondst van grote hoeveelheid gelekte inloggegevens met schoolaccounts.

In mei 2025 kreeg School-CERT van het Nationaal Cyber Security Centrum (NCSC) toegang tot een lijst met een groot aantal gelekte inloggegevens van diverse platforms, waarbij schoolaccounts als gebruikersnamen waren gebruikt. Deze gegevens werden gevonden tijdens Operation Endgame, een doorlopende samenwerking van internationale politiediensten waarbij servers en botnets van cybercriminelen offline worden gehaald.[12] De gestolen gegevens waren onder andere buitgemaakt door infostealers die op apparaten van de getroffen gebruikers waren terechtgekomen.

De lijst die School-CERT ontving, bevatte ongeveer 4.000 account-gegevens. Het plan was om zoveel mogelijk scholen op de hoogte te stellen van hun gelekte gebruikersaccounts. Naast een handelingsperspectief voor de gelekte accountgegevens, werd informatie gegeven over infostealers en hoe je die kunt tegengaan. De grootste uitdaging was de grote hoeveelheid gelekte data, waardoor School-CERT moest afwijken van de vaste werkwijze. Zo kostte het veel tijd om de contactgegevens te vinden van scholen die nog niet bij School-CERT zijn aangesloten. Zoveel mogelijk schoolbesturen laten aansluiten bij School-CERT de komende jaren is dus een belangrijk doel. Zo kan iedereen op tijd worden gewaarschuwd. Infostealers zijn binnen het onderwijs, net als in andere sectoren, een toenemende dreiging.

Wat ziet School-CERT?

Ook School-CERT heeft de dreiging van infostealers op de radar. In de kwartaalanalyse van School-CERT van zomer 2025 is het onderwerp infostealers uitgediept en toegelicht. School-CERT kreeg bovendien te maken met een groot incident dat te herleiden is naar het gebruik van infostealers door criminelen.

School-CERT erkent de aanwezigheid van infostealers en de gevaren ervan, maar ziet ook dat het opmerken van de aanwezigheid van deze dreiging heel lastig is. Als een infostealer op een apparaat zit, ervaart de gebruiker daar namelijk niet direct de impact van, zoals dat wel bij een DDoS-aanval of een phishingbericht het geval is. Daardoor is het moeilijk om een volledig beeld te vormen van de dreiging. In het bredere cyberlandschap ziet School-CERT wel een toename van het gebruik van infostealers door criminelen in verschillende sectoren. Ook andere CERTs zien en erkennen dit probleem.[13]

Volgens onderzoek van het Canadese cybersecuritybedrijf eSentire,[14] is er een stijging van 156% identiteitsgerelateerde cyberaanvallen (aanvallen gericht op gebruikersgegevens en identiteit) gezien tussen 2023 en 2025. In het eerste kwartaal van 2025 werd 35% van deze aanvallen gedaan met infostealers, tegen 11% twee jaar eerder.

12 *Internationale politiediensten pakken met Operation Endgame door in bestrijding ransomware, politie*

13 *Infostealer malware in opmars: zo herken en voorkom je digitale dataroof, SURF*

14 *Identity-Centric Threats: The New Reality, 2025, eSentire*

Deze toename is te verklaren door het toenemende aanbod van infostealers als Malware-as-a-Service. Dit betekent dat mensen een malwarepakket kunnen kopen en inzetten voor een maandelijks bedrag. Hierdoor kunnen aanvallers met geringe technische kennis ook eenvoudig infostealers inzetten.[15]

Hoe kan jouw bestuur zich voorbereiden op deze dreiging?

Infostealers komen je systeem via onbetrouwbare downloads, phishing-mails en nep-CAPTCHA's. De beste manier om je hiertegen te beschermen is door alert te zijn op hoe je digitaal te werk gaat. Wees alert op phishingmails en op nep-CAPTCHA's. Het advies is om alleen software van de officiële bronnen te downloaden. Door software te downloaden die niet van officiële bronnen komt, heb je kans dat er een infostealer meekomt.

Om te voorkomen dat een infostealer toegang krijgt tot je gegevens, is het aan te raden om een wachtwoordmanager te gebruiken en je wachtwoorden niet in je browser op te slaan. De wachtwoorden in je browser zijn voor een infostealer namelijk gemakkelijk te benaderen en daarmee kunnen al je opgeslagen wachtwoorden gestolen worden.

Ook zijn er technische maatregelen die je kunt nemen om de gevolgen van infostealers te beperken, zoals goede beveiliging op je apparaten - ook wel endpoint-security genoemd - en DNS-filtering op je firewall.

DNS-filtering kan kwaadaardige domeinen blokkeren, zodat de infostealer op jouw apparaat geen contact kan maken met de computer van de aanvaller. Daarnaast hebben veel firewalls een continu bijgewerkte lijst van veelvoorkomende malwaredomeinen die automatisch kunnen worden geblokkeerd.

Het Groeipad bij het Normenkader IBP biedt handvatten om aan de slag te gaan met deze informatie. Voor deze dreiging kun je kijken naar de volgende deelprojecten:

- *Deelproject 2.3 – Bewustwording creëren*
- *Deelproject 2.4 – Omgaan met incidenten en datalekken*
- *Deelproject 3.1 – Veilig beheer van infrastructuur*
- *Deelproject 3.6 – Beveiligen van werkplekken en mobiele apparaten*

Incidenten in de media

Op 23 mei 2025 meldde de Nederlandse politie dat ze in samenwerking met internationale opsporingsdiensten meerdere botnets offline hebben gehaald.[16] Bij deze grote operatie, Operation Endgame 2.0, werden meer dan 300 servers offline gehaald, waardoor de criminelen geen toegang meer hadden tot hun systemen. Ook de infostealer Lumma, een van de grootste op dat moment, werd offline gehaald. Tijdens deze actie werden er datasets aangetroffen met gestolen inloggegevens van Nederlandse gebruikers.

15 *Malware-as-a-Service goed voor meer dan de helft van de cyberdreigingen, Dutch IT Channel*

16 *Internationale politiediensten pakken met Operation Endgame door in bestrijding ransomware, politie.nl*

School-CERT ontving van het NCSC (Nationaal Cyber Security Centrum) een lijst met gebruikers uit deze datasets die te herleiden waren naar een Nederlandse organisatie in het primair en voortgezet onderwijs. Op basis van deze informatie heeft School-CERT contact opgenomen met veel Nederlandse instellingen om hen te informeren over de gelekte gegevens, zodat zij snel maatregelen konden nemen.

Ook de aanval op TU Eindhoven in de eerste maand van 2025 is volgens bronnen terug te leiden naar een infostealer.[17] Door diefstal van gegevens van ten minste één medewerker en één student, kregen de aanvallers toegang tot de systemen van TU Eindhoven. Dit stelde hen in staat zich verder door de organisatie te bewegen, waardoor de universiteit zelf besloot om het volledige systeem offline te halen. Hierdoor kon er tijdelijk geen les worden gegeven en moesten tentamens worden uitgesteld.[18]

17 *Aanval TU Eindhoven begon bij 'infostealer': software die van alles steelt, NOS*

18 *Hacker had dagenlang ongemerkt toegang tot netwerk TU Eindhoven, NOS*

Phishing

Phishing is een vorm van digitale fraude waarbij social engineering wordt toegepast om toegang te krijgen tot vertrouwelijke gegevens en systemen. Social engineering is een techniek waarbij aanvallers misbruik maken van menselijke eigenschappen als vertrouwen, nieuwsgierigheid, angst of behulpzaamheid. Aanvallers die zich op het primair en voortgezet onderwijs richten, verschuiven hun aandacht steeds meer naar dit menselijke element in de beveiligingsketen.[19]

Met de komst van digitale communicatieplatforms kan phishing op allerlei manieren plaatsvinden, zoals via e-mail, social media of via een app-bericht, maar ook nog steeds telefonisch. Phishingberichten zijn onverwacht of ongewoon. Soms hebben ze een ongebruikelijke afzender, maar vaak lijkt het alsof de berichten van een betrouwbare bron komen, zoals een betrouwbare organisatie of een bekend persoon. Het misleiden van iemand, door zich voor te doen als een ander, wordt *spoofing* genoemd.[20] Aanvallers kunnen bijvoorbeeld het afzenderadres van een e-mail vervalsen en zich voordoen als leveranciers, (oud-)medewerkers, leerlingen of ouders.

Zo kan iemand een bericht ontvangen met een link naar een website waarop moet worden ingelogd om een belangrijk document te bekijken. De afzender en de website lijkt betrouwbaar, waardoor de inloggegevens in handen komen van de aanvaller. Ook kunnen criminelen berichten met besmette bijlagen versturen.

19 *2025 CIS MS-ISAC K-12 Cybersecurity Report: Where Education Meets Community Resilience, 6 maart 2025, CIS*

20 *Cybersecurity Woordenboek. Van cybersecurity naar Nederlands, 2e druk, Cyberveilig Nederland*

Wanneer zo'n bijlage wordt geopend, wordt malware geïnstalleerd die de aanvaller toegang geeft tot het schoolsysteem. Een succesvolle phishingaanval leidt op die manier tot een datalek en kan het begin zijn van een ransomwareaanval (zie het hoofdstuk over ransomware).

Een phishingbericht waar relevante informatie aan is toegevoegd om een specifieke persoon te misleiden wordt *spear phishing* genoemd. Dit soort berichten zijn moeilijker te herkennen als een aanval.[21] *Spear phishing* is vaak gericht op het direct uitvoeren van transacties, zoals het overmaken van geld of het aanpassen van een toetsresultaat.

Phishing kan in verband worden gebracht met andere vormen van fraude, zoals:

- **Identiteitsdiefstal:** het stelen van persoonlijke gegevens, met de bedoeling deze te gebruiken voor fraude of andere illegale activiteiten.
- **Identiteitsfraude:** het opzettelijk gebruiken van iemands persoonlijke gegevens zonder toestemming, bijvoorbeeld om in een systeem in te breken of om aankopen te doen op kosten van een ander.
- **Business e-mail compromise:** de aanvaller is doorgedrongen tot de mailomgeving van een organisatie en kan zo vertrouwelijke informatie stelen of CxO-fraude uitvoeren.
- **CEO/CFO/CxO-fraude:** een specifieke vorm van business e-mail compromise, waarbij de aanvaller e-mails verstuurt uit naam van een bestuurder met als doel een medewerker onder druk te zetten om geld over te maken.

21 *Cybersecurity Woordenboek. Van cybersecurity naar Nederlands, 2e druk, Cyberveilig Nederland*

Uit de praktijk

Fraudeur doet dure bestellingen uit naam van schoolbestuur Innoord met een vals e-mailadres en verstuurt verdachte e-mails.

In 2025 kreeg Innoord, het schoolbestuur van alle openbare basisscholen in Amsterdam Noord, op de vrijdag voor de voorjaarsvakantie een telefoontje van een leverancier over een bestelling van een 3D-printer. Het e-mailadres dat voor de bestelling was gebruikt, leek van een van de scholen van Innoord te zijn, maar niemand op die school was op de hoogte van de bestelling. Uit nader onderzoek bleek dat het e-mailadres waarmee de bestelling was geplaatst eindigde op .com in plaats van het gebruikelijke .nl. De leverancier annuleerde de bestelling.

Tijdens de voorjaarsvakantie kreeg het secretariaat van Innoord meer telefoontjes van leveranciers over bestellingen, waaronder printers en jassen. Opvallend was dat de naam van een oud-schooldirecteur werd genoemd. Ook had de fraudeur bewust aangegeven dat de bestellingen op een ander adres mochten worden geleverd vanwege de vakantie. Dankzij de oplettendheid van de leveranciers was dit nog niet gebeurd, maar de situatie bleef zorgwekkend. Toen na de vakantie vergelijkbare meldingen bleven binnenkomen, besloot Innoord actie te ondernemen.

Een projectteam werd samengesteld, bestaande uit de bestuurssecretaris, het hoofd bedrijfsvoering en de bovenschoolse ICT'er. Naast de frauduleuze bestellingen bleken er ook verdachte mails te worden verstuurd uit naam van een oud-medewerker en was er een poging gedaan om via de Kamer van Koophandel een

wachtwoord aan te passen. Het projectteam schakelde School-CERT in voor advies over een plan van aanpak, zowel op technisch vlak als op het gebied van communicatie. Bestuurssecretaris bij Innoord Sophie Pennington de Jongh zegt hierover:

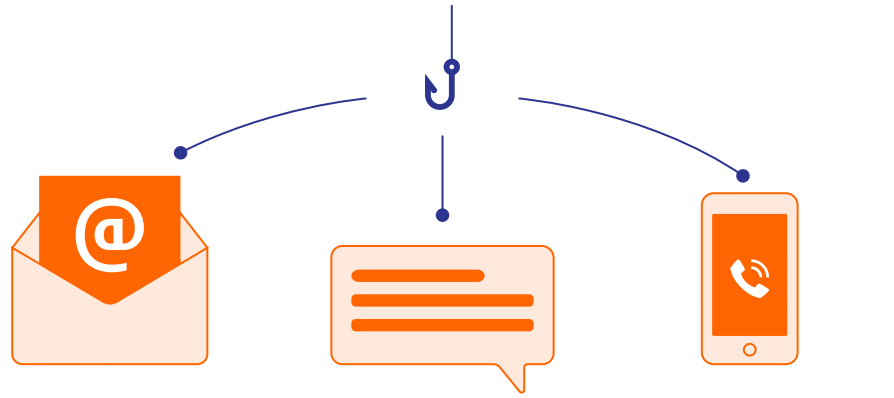
“We zijn gestart met de interne communicatie: we hebben direct onze directeuren, administratief medewerkers en de collega’s van de financiële afdeling gevraagd om extra voorzichtig om te gaan met facturen.

“Diezelfde dag hebben we alle medewerkers een mail gestuurd om hen te informeren en te waarschuwen. Het was misschien nog wel belangrijker voor ons om hen gerust te stellen. Zij moesten geen enkele drempel voelen om naar ons toe te komen, juist als ze per ongeluk iets verdachts hadden goedgekeurd of een verkeerde link hadden aangeklikt.

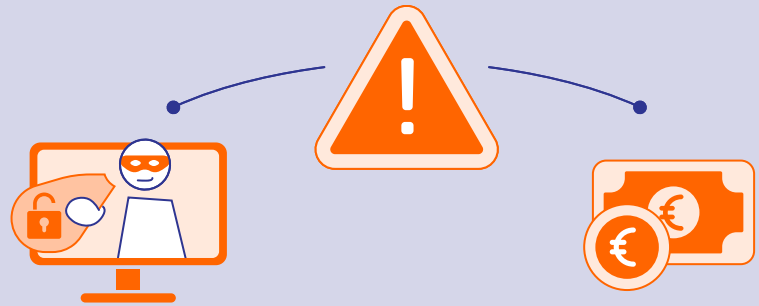
“Op de contactpagina van onze website hebben we een zin toegevoegd om leveranciers te vragen alert te zijn bij bestellingen van Innoord. Op advies van School-CERT hebben we bovendien aangifte gedaan bij de politie. Ten slotte hebben we de oud-collega’s van wie de namen in de frauduleuze mails werden gebruikt, geïnformeerd en nazorg aangeboden.”
Ondanks deze maatregelen bleek dat één leverancier toch een printer ter waarde van enkele duizenden euro’s had laten uitleveren op een adres een kilometer bij Innoord vandaan. In dit geval heeft dit uiteindelijk niet tot schade geleid voor het school-bestuur en hebben zij de bestelgegevens doorgegeven aan de politie.

Nadat de politie aangaf geen verder onderzoek te kunnen doen, zorgde School-CERT ervoor dat de frauduleuze mailadressen offline werden gehaald. Ook werd bij de ICT-leverancier nagegaan of er kwetsbaarheden of verdachte activiteit waren, wat gelukkig niet het geval bleek te zijn.

Phishing



Gevolgen



Wat ziet School-CERT?

Cybercriminelen slaan, zoals ook in dit voorbeeld, vaak toe net voor of tijdens een schoolvakantie. In deze periodes zijn er minder mensen aan het werk, waardoor fraude langer onopgemerkt kan blijven.
In het genoemde voorbeeld werd de vakantieperiode daarnaast als reden gebruikt om de bestellingen naar een ander adres te kunnen versturen. Toetsperiodes zijn andere momenten waarop cybercriminelen actief zijn, omdat ze dan extra druk kunnen uitoefenen op medewerkers. Als toetsen niet kunnen doorgaan omdat de benodigde systemen onbereikbaar zijn, zorgt dat immers voor veel onrust bij leerlingen en ouders.

In het voortgezet onderwijs zien we bovendien voorbeelden van fraude door leerlingen. Ze willen bijvoorbeeld hun cijfers aanpassen, gratis gebruikmaken van software of het account van een leraar overnemen om toegang te krijgen tot toetsinformatie. Ook bij cyberpesten kan fraude een rol spelen, zoals wanneer leerlingen inbreken in het account van een klasgenoot om opzettelijk fouten in diens opdrachten te maken.

Als een phishingbericht leidt tot een datalek of een ramsomware-aanval heeft dat grote gevolgen voor een school. Denk aan de hoge kosten voor de (technische) ondersteuning die nodig is om de aanval te onderzoeken en te stoppen. Bovendien kan het de continuïteit van het onderwijs en het imago van de instelling negatief beïnvloeden.

Hoe kan jouw bestuur zich voorbereiden op deze dreiging?

Er zijn verschillende maatregelen die de kans op een phishingaanval verkleinen, maar je kunt het nooit helemaal voorkomen. Dit komt onder andere door de opkomst van technologieën als AI, die phishingberichten steeds geloofwaardiger kunnen maken. Het is daarom belangrijk om te werken aan bewustwording, voorlichting en duidelijke gedragsregels. Zorg bijvoorbeeld voor een toegankelijk meldpunt waar medewerkers en leerlingen verdachte berichten kunnen melden.

Technische maatregelen kunnen de kans verkleinen dat phishing-berichten via e-mail bij medewerkers of leerlingen terechtkomen.
Je kunt filters gebruiken en waarschuwingen instellen voor berichten van en naar externen.[22] Met webfiltering kun je ervoor zorgen dat medewerkers automatisch worden tegengehouden als ze op een link naar een gevaarlijke website klikken.

Daarnaast zijn er technische maatregelen die kunnen voorkomen dat phishingberichten vanuit jouw domein kunnen worden verzonden. Beveiligingsinstellingen zoals SPF, DKIM en DMARC helpen bij het beschermen van je domeinnaam.

Deze verificatiemethoden zorgen ervoor dat alleen geautoriseerde mailservers berichten vanuit jouw domein mogen versturen. Ook kun je limieten instellen voor het aantal ontvangers van e-mailberichten die vanuit jouw organisatie worden verzonden.

---

22 Veilig omgaan met e-mail op jouw school: vijf maatregelen, Kennisnet

Zorg voor sterke digitale basismaatregelen, vooral voor belangrijke systemen zoals het leerlingvolgsysteem. Bij het kiezen van een leverancier kun je het *Certificeringsschema informatiebeveiling en privacy ROSA* en het *privacyconvenant* raadplegen. Ook is er *Edu-V*, een keurmerk voor digitale gegevensuitwisseling in het onderwijs, en een *Edustandaard* voor veilig en betrouwbaar mailverkeer.

Zorg er altijd voor dat systemen up-to-date blijven en gebruik waar mogelijk multifactorauthenticatie (MFA). Mocht er toch een phishing-aanval plaatsvinden, gebruik dan de *handreiking van School-CERT* voor hulp bij een phishingaanval.

Normenkader IBP en Groeipad

- *Deelproject 2.3 – Bewustwording creëren*
- *Deelproject 2.4 – Omgaan met incidenten en datalekken*
- *Deelproject 2.7 – Beveiligingseisen en -maatregelen vastleggen in een beveiligingsbaseline*
- *Privacy domein 6: Beveiliging*
- *Informatiebeveiliging domein 6: Incident- en problemmanagement*

Incidenten in de media

Onderzoek toont aan dat phishingberichten traditionele technische veiligheidsmaatregelen kunnen omzeilen, waardoor de mens een belangrijke factor blijft binnen de beveiligingsketen.[23]

Als gevolg van *spear phishing* werden in Edinburg schoolnetwerken offline gehaald en moesten leerlingen op zaterdag naar school komen om hun wachtwoord te resetten.[24]
Mailaccounts van scholen en bedrijven worden overgenomen en gebruikt om via phishingberichten kwaadwillende software te verspreiden.[25]

23 *Ruim helft phishing-e-mails omzeilt alle lagen van beveiliging, ChannelConnect*
24 *Exam revision disrupted as cyber attackers target Edinburgh council, BBC*
25 *The New Face of Remcos Malware, Forcepoint*

Ransomware

Ransomware is een dreiging met een grote impact op de organisatie en mensen die het overkomt. Wanneer jouw school wordt getroffen door ransomware, worden systemen en bestanden versleuteld en wordt data buitgemaakt. In het Nederlands wordt ransomware ook wel gijzelsoftware genoemd, omdat informatie van een organisatie wordt gegijzeld door kwaadwillende hackers. De hackers benaderen een organisatie en eisen losgeld.

Voorheen werd dit losgeld vaak geëist in ruil voor het terugkrijgen van bestanden, maar tegenwoordig hebben organisaties vaak goede back-ups. Daarom hebben ransomwaregroepen hun strategie aangepast en dreigen ze nu vaak gevoelige informatie openbaar te maken als je niet betaalt. De informatie wordt dan op het dark web geplaatst of op eigen websites, zogenaamde *leaksites*.

Ransomware is een van de meest ingrijpende en kostbare vormen van malware, omdat het op grote schaal de processen van organisaties verstoort. Het is na een ramsomwareaanval niet mogelijk om op de normale manier te werken en toegang tot belangrijke informatie gaat verloren. De mogelijkheid om onderwijs te geven is meestal wel sneller hersteld. Het herstel van een ransomwareaanval duurt gemiddeld drie tot zes weken en brengt flinke kosten met zich mee. Vaak moet een deel van het netwerk opnieuw worden opgebouwd, zelfs wanneer er goede back-ups zijn. De impact op medewerkers is ook fors, omdat er vaak gevoelige gegevens over henzelf of hun leerlingen worden buitgemaakt. Scholen staan ook voor de moeilijke keuze om al dan niet te betalen aan de ransomwaregroep. School-CERT adviseert om niet te betalen, omdat je met een betaling het verdienmodel achter ransomware in stand houdt.

Uit de praktijk

Accountmanager Cybercrime ziet toename van ransomware en ransomwaregroepen die zich steeds meer specialiseren.

Accountmanager Cybercrime van de Politie Oost-Brabant Onno Sidler ziet bij politiezaken met ransomware op scholen in de meeste gevallen dat mbo's, hbo's en universiteiten getroffen worden. Scholen in het primair en voortgezet onderwijs zitten er wel tussen, maar veel minder. Hackers kiezen er vaak ook niet specifiek voor om een school te hacken. Vaak schieten ze met hagel en raken daarbij soms een school. Pas als ze binnen zijn, kijken ze wat ze hebben en wat ze ermee kunnen. Het is tegenwoordig niet zozeer de vraag óf een school slachtoffer wordt, maar wanneer. Als ze bij een school binnenkomen, is dat vaak op bestuursniveau. Meestal maken meerdere scholen gebruik van hetzelfde netwerk, waardoor meerdere scholen tegelijk kunnen worden getroffen.

Over het algemeen ziet hij steeds vaker dat er ransomware wordt uitgevoerd waarna gedreigd wordt de buitgemaakte gegevens te publiceren. Dit noemen we in politietermen ook wel afdreiging. Het is dus niet meer 'geef ons geld dan krijg je je data terug', maar 'geef ons geld anders gooien we je informatie online'. Reputatieschade is vaak een effectief middel.

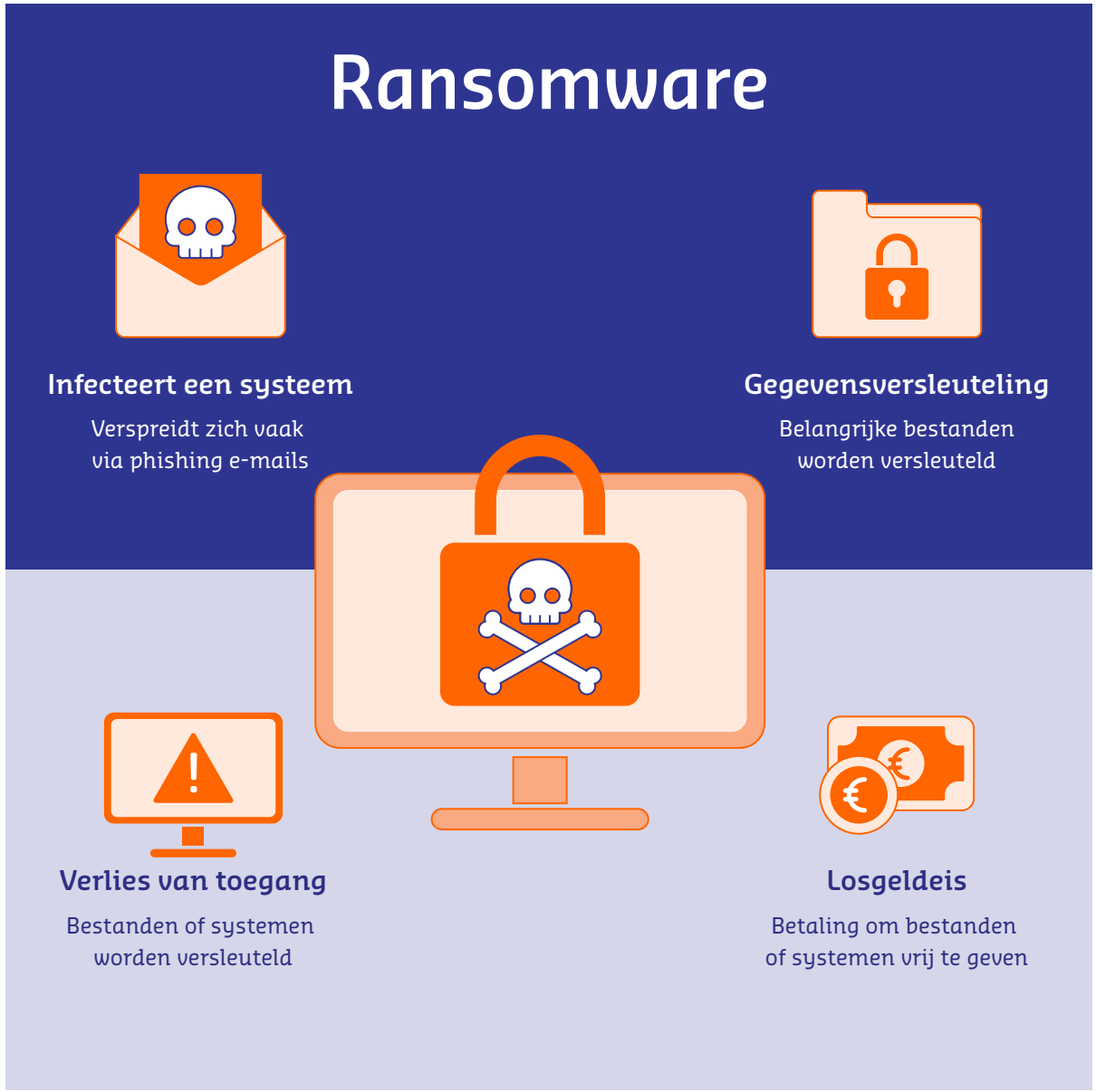
De informatie wordt niet alleen op het dark web gepubliceerd, maar ook op zogeheten *leaksite*s. Dit zijn websites waar ransomwaregroepen de buitgemaakte data van slachtoffers tonen.
De politie houdt deze *leaksites* in de gaten en waarschuwt als daar Nederlandse slachtoffers op langskomen.

Ook constateert hij dat ransomwaregroepen zich steeds meer specialiseren. Zo richten ze zich bijvoorbeeld op het verkrijgen van toegang tot systemen en verkopen die toegang aan zogeheten affiliates: degenen die deze toegang vervolgens gebruiken om ransomware te verspreiden.

Een ander voorbeeld van specialisatie was het geval van iemand die werd aangehouden omdat hij een speciale bot had ontwikkeld. Met deze bot kon bijvoorbeeld een telefoontje worden gepleegd namens een bank laten om een klant te laten weten dat iemand probeert diens rekening te hacken.
Een babbeltruc dus, waarbij je geen echte persoon aan de lijn krijgt, waardoor je ook geen kritische vragen kunt stellen. Doordat de computerstem overkomt over als een autoriteit, waren mensen waren eerder geneigd hun controle-code of eenmalig wachtwoord te delen.

Uitbesteden is niet per se veiliger. Dat maakt je afhankelijk van de partij aan wie je het hebt uitbesteed. Of de data nou in de cloud staat of lokaal, als je binnen kunt komen kun je de data alsnog stelen.

Onno Sidler, Accountmanager Cybercrime Publiek Private Samenwerking bij de Politie Oost-Brabant adviseert: "Als je van huis gaat en je laat de sleutel in het slot zitten, kun je nog zo'n goed slot hebben, maar dan heeft dat geen zin. Gebruik dus niet overal hetzelfde wachtwoord, zorg voor goede basisbeveiliging en neem gebruikers ook goed mee. Door alle tooltjes die tegenwoordig beschikbaar zijn, is hacken laagdrempeliger geworden."


Ransomware
Infecteert een systeem
Verspreidt zich vaak
via phishing e-mails
Gegevensversleuteling
Belangrijke bestanden
worden versleuteld
Verlies van toegang
Bestanden of systemen
worden versleuteld
Losgeldeis
Betaling om bestanden
of systemen vrij te geven

Wat ziet School-CERT?

In de afgelopen twee jaar zijn verschillende scholen en IT-leveranciers voor het onderwijs slachtoffer geworden van ransomware. Sinds de lancering van School-CERT op 15 oktober 2024 zijn er drie meldingen van getroffen scholen binnengekomen, waarvan er één bij nader onderzoek vals alarm bleek te zijn. In alle gevallen was de continuïteit van het onderwijs slechts relatief kort verstoord, maximaal enkele dagen. Dit komt doordat voor de toegang tot lesmateriaal meestal alleen een internetverbinding nodig is.

De gevolgen voor de rest van de organisatie zijn veel groter, omdat bijvoorbeeld personeelsgegevens worden gestolen en openbaar kunnen worden gemaakt. Vaak blijkt er meer persoonlijke informatie van medewerkers lokaal opgeslagen te zijn dan verwacht. Daarnaast staat leerlinginformatie regelmatig buiten de aangewezen Leerling Adminstratie Systemen (LAS). Het kan ook voorkomen dat het les-proces niet is verstoord, maar andere onderwijsprocessen dat wel zijn.

Hoe kan jouw bestuur zich voorbereiden op deze dreiging?

Het is moeilijk om ransomware volledig te voorkomen, maar er zijn verschillende maatregelen die je kunt nemen om de kans op een succesvolle aanval te verkleinen. En door een goede voorbereiding kan de duur van de verstoring van processen worden teruggebracht.

Voorkomen van een geslaagde aanval

Twee maatregelen hebben in de gevallen waarbij School-CERT betrokken was, de schade beperkt: multifactorauthenticatie (MFA) en beperken van rechten.

MFA maakt het moeilijker voor een kwaadwillende hacker om een account over te nemen. Het is echter wel van belang welke vorm van MFA je gebruikt, want steeds meer hackers slagen erin de authenti-catiecode te onderscheppen door hun slachtoffer te manipuleren.

Door MFA te combineren met het beperken van de rechten van accounts, kan de schade voor de organisatie nog verder worden verminderd. De stap met de meeste positieve impact is het beperken van het aantal accounts met adminrechten. Deze rechten stellen gebruiker in staat om wijzigingen aan te brengen op systemen en niet-goedgekeurde applicaties te downloaden. Hoe meer medewerkers adminrechten hebben, hoe groter de kans is voor een kwaadwillende om succesvol de school te hacken. De systemen van jouw organisatie kunnen worden overgenomen, als het wachtwoord van iemand met deze rechten op straat komt te liggen of die persoon op een verkeerde link klikt.

Wil je hiermee aan de slag, zie dan:
Deelproject 3.2 Inrichten van identiteits- en toegangsbeheer

Schade beperken

Deze maatregelen kunnen helaas niet alle ransomwareaanvallen voorkomen. Er zijn verschillende voorbereidingen die je kunt treffen om de schade te beperken. Door in kaart te brengen wat de kroon-juwelen van jouw organisatie zijn, kun je bepalen waar de focus moet liggen bij de informatiebeveiliging. Kroonjuwelen zijn de belangrijkste processen binnen jouw organisatie en de systemen die ervoor nodig zijn om die processen uit te voeren, zoals het uitbetalen van salarissen of het waarborgen van de continuïteit van het onderwijs. Een duidelijk overzicht van systemen die cruciaal zijn voor kritieke

processen helpt richting te geven aan je plannen voor bedrijfscontinuïteit en incidentmanagement. Ook een goed plan voor back-up en herstel is van groot belang, aangezien dat de basis vormt van het opnieuw opbouwen van het netwerk na een aanval. Onderstaande deelprojecten kunnen daarbij helpen. School-CERT heeft een handreiking voor hulp bij ransomware beschikbaar gesteld met een stappenplan dat helpt grip te houden op de acties die je moet ondernemen bij een ransomwareaanval.

- *Deelproject – 2.10 Waarborgen van bedrijfscontinuïteit*
- *Deelproject – 2.4 Omgaan met incidenten en datalekken*
- *Deelproject – 2.11 Back-up en herstel van gegevens*
- *School-CERT handreiking Hulp bij een ransomewareaanval*

Incidenten in de media

Situatie in Groot-Britannië waarbij 143 scholen en kinderdagverblijven werden getroffen door ransomware op het onderwijssysteem van hun council.[26]

Scholengroep wordt getroffen door ransomware en sluit uiteindelijk een deal met de kwaadwillende hackers.[27]
Media kwamen achter de aanval op deze school, omdat hun informatie op het dark web werd aangetroffen.[28]

26 *West Lothian schools hit by ransomware attack, Digital Watch Observatory*

27 *Scholengemeenschap OSG Hengelo sluit deal met hackers na ransomware-aanval, 1Twente*

28 *Middelbare school Het Rhedens getroffen door ransomware, Dutch IT Channel*

Conclusies en aanbevelingen

Conclusie

Er komen veel dreigingen op het onderwijs af. Scholen worden steeds afhankelijker van cloudtechnologie die ze zelf afnemen of die wordt gebruikt door leveranciers. School-CERT merkt op dat zowel de kans op een aanval als de impact van een succesvolle aanval is toegenomen. Naast de zichtbare verstoringen, zoals ransomware, verdienen ook de niet-zichtbare storingen, zoals infostealers, aandacht. De detectie en preventie voor deze dreigingen blijven op dit moment achter.

Cyberdreiging beheersen is een hoofdzaak, geen bijzaak!

Tegelijk ziet School-CERT dat scholen zich meer bewust worden van het nut van cybersecurity en dat er actief wordt gewerkt om de cyberveiligheid van scholen te verbeteren. Desondanks blijven scholen in de breedte kwetsbaar voor aanvallen. De mensen, de gebruikte systemen en de afhankelijkheid van leveranciers blijven hierbij zwakke plekken. Doordat de middelen om cyberaanvallen uit te voeren eenvoudiger te maken of te verkrijgen zijn, is het belangrijk dat scholen actief bezig blijven om hun cyberveiligheid te verhogen. Scholen hebben hier in veel gevallen beperkte middelen en tijd voor. School-CERT speelt een cruciale rol in het verhogen van de cyberveiligheid. Zij informeren en adviseren de sector over incidenten, dreigingen en kwetsbaarheden. Dit zorgt ervoor dat scholen met minder middelen en expertise ook op de hoogte worden gesteld van zaken die impact kunnen hebben op het onderwijs.

Aanbevelingen

Op basis van de waargenomen dreigingen en adviezen volgen hier drie aanbevelingen om de weerbaarheid en veerkracht van de sector te verbeteren. Hoewel deze aanbevelingen misschien als vanzelfsprekend klinken, zijn ze volgens School-CERT fundamenteel voor het beheersbaar houden van cyberdreiging en het omgaan met aanvallen.

Voorbereiding is het halve werk

Voorbereid zijn op een aanval is net zo belangrijk als het voorkomen ervan. De voorbereiding omvat draaiboeken met verantwoordelijkheidsafspraken, contactlijsten en het bewaken van (juridische) deadlines. Dit kunnen korte documenten zijn die houvast bieden tijdens een crisis.

Een crisisoefening organiseren op school helpt je om beter te reageren op een echte cyberaanval. Door te oefenen, weet je als team wat je moet doen en kun je sneller en effectiever handelen in een echte crisissituatie. Dit kan de schade beperken en de tijd verkorten die nodig is om weer normaal te functioneren. Tijdens een oefening kunnen bovendien zwakke punten in de crisisreactie van jouw organisatie aan het licht komen. Door periodiek te oefenen, weet iedereen wat er van hem/haar verwacht wordt. Bekijk de informatie en oefenpakketten op de *website van Kennisnet*.

Een ander aspect van voorbereiding is het hebben van een compleet programma van eisen. Vaak zijn deze programma's te veel gericht op de primaire, functionele wensen en eisen en worden de eisen voor cyberweerbaarheid niet meegenomen. In dienstverleningsovereenkomsten worden verantwoordelijkheden (taken en kwaliteitsdoelstellingen) vaak onvoldoende concreet uitgewerkt.

Vergeet niet dat het schoolbestuur altijd eindverantwoordelijk blijft voor de verwerking van data door cloud- of dienstleverancier, inclusief internetproviders.

Een gedegen voorbereiding helpt de kans op aanval te verkleinen en de impact te beperken.

Samen werken is samen sterker

Door samenwerking en het delen van kennis en capaciteit kan de benodigde inspanning voor cyberweerbaarheid worden gedeeld en verdeeld. Dit kan de kwaliteit van ICT-onderwijsproducten of -diensten in de gehele levenscyclus verbeteren, mogelijk tegen lagere kosten.

Samenwerking met andere schoolbesturen kan de weerbaarheid versterken. Daarnaast is er het programma Digitaal Veilig Onderwijs (DVO) met onder andere School-CERT, het Normenkader IBP en het Groeipad.

Open cultuur

Zorg voor een veilige interne omgeving. Maak medewerkers bewust van het feit dat zij een doelwit kunnen zijn. Maak het eenvoudig om ongebruikelijke e-mails en situaties te melden. Door deze meldingen als schoolbestuur ook door te geven aan School-CERT, kan de sector beter en sneller worden geïnformeerd over cyberdreigingen.

Een snelle respons kan de impact van een aanval beperken.

Vervolg

Het vervolg op dit dreigingsbeeld omvat het uitvoeren of bijwerken van een risicoanalyse. Dit zal duidelijk maken welke dreigingen voor jouw school het meest relevant zijn welke impact je moet verwachten. Vergeet niet om na een training of aanval een evaluatie te doen; dit is belangrijk voor het proces van continue verbetering. Vanuit het programma DVO, met onder andere School-CERT en het Normenkader IBP, wordt er ondersteuning geboden.

Meer informatie

- Het Normenkader Informatiebeveiliging en Privacy helpt scholen om de digitale veiligheid te verhogen. Zodat leerlingen, ouders en medewerkers erop kunnen rekenen dat zij leren en werken in een digitaal veilige schoolomgeving en dat hun persoonsgegevens goed worden beschermd. Kijk op: *kn.nu/overhetnormenkader*
- Met het Groeipad ga je projectmatig en stapsgewijs aan de slag met het bereiken van volwassenheidsniveau 3 van het Normenkader IBP. *Kijk op: kn.nu/groeipad*

School-CERT

School-CERT is een sectoraal CERT voor het bekostigd primair en voortgezet onderwijs in Nederland. CERT staat voor Computer Emergency Response Team. Het is een gespecialiseerd team van ICT-professionals, dat in staat is snel te adviseren in het geval van een cybersecurity-incident.

School-CERT bestaat sinds oktober 2024 en wordt uitgevoerd door Kennisnet in samenwerking met SIVON. School-CERT wordt gefinancierd door het ministerie van Onderwijs, Cultuur en Wetenschap (OCW).

Waarom deelnemen aan School-CERT?

Samen staan we sterker. Door met elkaar (anoniem) informatie te delen over cybersecurity-kwetsbaarheden en incidenten binnen de onderwijssector helpen we elkaar. School-CERT zet zich in voor de continuïteit van het onderwijs. De experts van School-CERT bieden ondersteuning tijdens een cybersecurity-incident zodat het onderwijs zo snel en veilig mogelijk door de school kan worden hervat.

School-CERT adviseert je over de meest verstandige aanpak bij cybersecurity-incidenten. Hoe reageert jouw schoolbestuur op een cybersecurity-incident of tijdens een crisis? Door hier goed mee om te gaan voorkom je reputatieschade. School-CERT kan je hierbij adviseren.

School-CERT is betrouwbaar, pragmatisch en bezit specialistische kennis over cybersecurity in het onderwijs. De experts van School-CERT voorzien jou van cybersecurity-informatie die relevant is voor het onderwijs, zoals informatie over kwetsbaarheden. Ze geven aan of de informatie een hoge prioriteit heeft en wat je nu het beste kunt doen. School-CERT heeft een onafhankelijke positie ten opzichte van bijvoorbeeld leveranciers en producenten. Daardoor kan School-CERT spoedig en kritisch een oordeel en advies uitbrengen over een incident.

Wat doet School-CERT niet?

School-CERT biedt alleen online hulp en levert geen hulp op locatie. Ook bieden we geen forensische dienstverlening aan, voeren we geen ransomware-onderhandelingen en brengen wij nooit zelf wijzigingen aan in systemen. Dit blijft altijd de verantwoordelijkheid van een schoolbestuur. Op dit moment biedt het CERT nog geen 24 x 7 ondersteuning. Mocht een ernstig incident beginnen tijdens kantoor-tijden dan gaat de hulpverlening wel verder buiten kantoortijden en/ of in het weekend, maar het melden van een groot incident of crisis kan alleen tijdens kantoortijden.

Aanmelden

Schoolbesturen binnen het bekostigd funderend onderwijs kunnen zich gratis aanmelden. Wil jij je schoolbestuur aanmelden? Meld je dan *hier* als deelnemer aan.

Colofon

Dreigingsbeeld Cybersecurity primair en voortgezet onderwijs 2025

Datum van uitgave
September 2025

Auteurs
Ad Bresser
Yaniek Wiegman
Marit van Piggelen
Lisanne Nugteren
Sabine Marsé

Eindredactie
Nanda van Dijk

Vormgeving
Van Hulzen Communicatie

Over Kennisnet
Goed onderwijs legt de basis voor leven, leren en werken en daagt leerlingen en studenten uit om het beste uit zichzelf te halen. Dat vraagt om onderwijs dat inspeelt op sociale, economische en technologische ontwikkelingen. Kennisnet ondersteunt besturen in het primair onderwijs (po), het voortgezet onderwijs (vo) en het middelbaar beroepsonderwijs (mbo) bij een professionele inzet van ICT en is voor scholen de gids en bouwer van het ICT-fundament.

Kennisnet wordt gefinancierd door het ministerie van Onderwijs, Cultuur en Wetenschap (OCW).

kennisnet.nl

Kennisnet
Postbus 778
2700 AT Zoetermeer

T 0800 321 22 33
E support@kennisnet.nl
I kennisnet.nl