Kennisnet

Dreigingsbeeld Funderend Onderwijs

2023

Laat ict werken **voor het onderwijs**

Inhoudsopgave

Waarom is dit dreigingsbeeld relevant?

Het onderwijs is, net als vele andere sectoren, in toenemende mate afhankelijk van ict. Er wordt steeds meer gebruikgemaakt van digitale middelen voor het geven van onderwijs, voor administratieve processen wordt vaak een cloud-omgeving gebruikt en digitale systemen en schoolorganisaties verwerken persoonlijke informatie van leerlingen en medewerkers. Gegevens over leerlingen en studenten kunnen op straat komen te liggen en de continuïteit van het onderwijs kan in gevaar komen wanneer systemen niet meer benaderbaar zijn[1].

Schoolbesturen denken nogal eens dat cyberdreigingen voor hen niet relevant zijn en dat zij toch geen interessant slachtoffer zouden zijn. Daarbij onderschat men dat je geen doelwit hoeft te zijn om slachtoffer te worden[2]. Door de professionalisering van cybercrime (bijvoorbeeld *Ransomware-as-a-Service*[3, 4]) is het daarnaast makkelijker geworden om een cyberaanval uit te voeren. Je hoeft er geen diepgaande technische kennis voor te hebben, waardoor de drempel om ook kleinere organisaties aan te vallen lager wordt. Ook technologische ontwikkelingen, zoals artificial intelligence[5], kunnen invloed hebben op cyberdreigingen. Cyberdreigingen hoeven niet altijd van 'buiten' de school te komen, ook leerlingen zijn een relevante actor in het dreigingsbeeld voor het onderwijs. Ze proberen uit hoever ze kunnen komen in een systeem, maar hebben vaak beperkt inzicht in de consequenties van hun acties[6].

Scholen verwerken persoonsgegevens: van medewerkers, van hun leerlingen – die vaak minderjarig zijn – en van ouders van leerlingen. Er zijn steeds meer datastromen met gevoelige informatie over leerlingen. Scholen moeten hier zorgvuldig mee omgaan. Bestuurders zijn verantwoordelijk om dit op een veilige manier te doen. De Autoriteit Persoonsgegevens schetst in haar sectorbeeld over het onderwijs in 2021: *"De kwetsbare positie van kinderen vereist bovendien dat zij extra beschermd worden, zodat zij zich in een vrije en veilige (school)omgeving kunnen ontwikkelen. Dit maakt de bescherming van persoonsgegevens in de onderwijssector essentieel."*[7] Beveiliging van deze persoonsgegevens is daarmee enorm belangrijk.

1 *Kamerbrief over verhogen digitale veiligheid onderwijs en onderzoek | Kamerstuk | Rijksoverheid.nl*

2 *De basis op orde | NCSC Magazine*

3 *Ransomware as a Service (RaaS) | Definition (trendmicro.com)*

4 *Cybersecuritybeeld Nederland 2023 | Nationaal Coördinator Terrorismebestrijding en Veiligheid (nctv.nl)*

5 *Publicatie | Artificial intelligence dringt door tot alle lagen van de samenleving (kennisnet.nl)*

6 *Hack_Right | Strafblad voorkomen | Opportuun (openbaarministerie.nl)*

7 *Trends, risico's en aanbevelingen over de bescherming van persoonsgegevens bij digitalisering in het onderwijs | Autoriteit Persoongegevens*

Volwassenheid en digitale weerbaarheid

In april 2023 is het Normenkader Informatiebeveiliging en Privacy (IBP) voor het Funderend Onderwijs gepubliceerd. Een nulmeting bij een steekproef van 15 schoolbesturen op basis van sector, grootte en geografische spreiding laat zien dat geen enkel schoolbestuur binnen de steekproef op dat moment voldeed aan de normen[8]. Een lagere volwassenheid op informatiebeveiliging en privacy maakt scholen kwetsbaar: ze zijn een potentieel slachtoffer van cyberdreigingen doordat ze er minder weerbaar tegen zijn. Ook is er bij veel schoolorganisaties beperkt capaciteit en/of expertise op dit onderwerp. Dit maakt het implementeren van maatregelen om dreigingen tegen te gaan uitdagend. Het verhogen van de volwassenheid en weerbaarheid is belangrijk vanwege een groeiende ict-afhankelijkheid binnen scholen. Want als de internetverbinding wegvalt, of als cruciale systemen, zoals de digitale leeromgeving of het leeradministratiesysteem, niet toegankelijk zijn, heeft dit direct impact op de continuïteit van het onderwijs[9] en kan grote gevolgen hebben voor leerlingen en studenten.

Toename ransomware-aanvallen in onderwijs

Sophos, een internationaal cybersecuritybedrijf, deed een wereldwijd onderzoek naar ransomware in de onderwijssector (in 31 landen, waaronder Nederland). Zij zien in 2022 in alle onderwijsrichtingen een toename van ransomware-aanvallen ten opzichte van eerdere jaren[10]. 56% van de scholen in het funderend onderwijs gaf aan geraakt te zijn door ransomware, ten opzichte van 44% in het jaar ervoor. Daarnaast blijkt dat het aanvallers in het onderwijs vaker lukt om data te versleutelen dan in andere sectoren (72% versus 65% van de aanvallen). Ook uit het wereldwijde malware-dreigingenoverzicht van Microsoft komt de onderwijssector naar voren als een van de meest geraakte sectoren[11].

Een digitaal veilige schoolomgeving realiseren

Om deze dreigingen het hoofd te bieden, is het belangrijk om een digitaal veilige omgeving voor alle leerlingen te realiseren en cyberdreigingen en risico's te adresseren. Met deze publicatie wil Kennisnet schoolbesturen ondersteunen bij het in beeld krijgen van de dreigingen en risico's voor je schoolorganisatie. Deze publicatie is ontwikkeld als onderdeel van het programma Digitaal Veilig Onderwijs[12]. We beschrijven verschillende actuele cyberdreigingen die relevant zijn voor het funderend onderwijs en geven handvatten om met deze dreigingen om te gaan. Op basis van de dreigingen die zijn beschreven in deze publicatie, kun je door het uitvoeren van risicoanalyses bepalen welke dreiging voor jouw school het meest relevant is. Op de Aanpak IBP vind je het Normenkader IBP voor het Funderend Onderwijs[13]. Hierin staan voorbeeldmaatregelen die je tegen de dreigingen kunt nemen.

8 *Nulmeting Normenkader IBP: waar staat het funderend onderwijs met informatiebeveiliging? | Kennisnet*

9 *Programmaplan | Digitaal Veilig Onderwijs (DVO) 2023 (squarespace.com)*

10 *A Sophos Whitepaper. July 2022 The State of Ransomware in Education 2022*

11 *Cyberthreats, viruses, and malware | Microsoft Security Intelligence*

12 *www.digitaalveiligonderwijs.nl*

13 *Trends, risico's en aanbevelingen over de bescherming van persoonsgegevens bij digitalisering in het onderwijs | Autoriteit Persoongegevens*

Definities

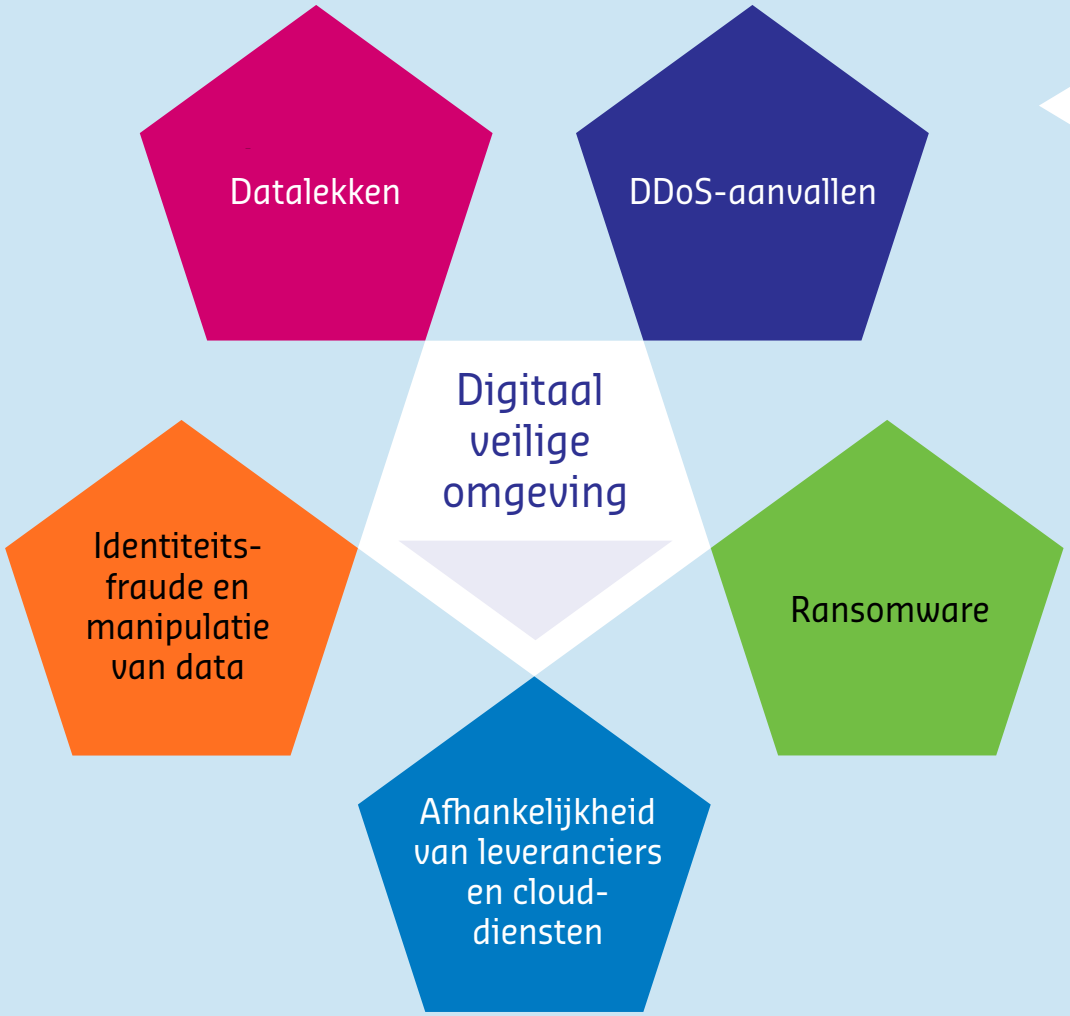
Voor het dreigingsbeeld voor het funderend onderwijs hanteren wij verschillende sleutelbegrippen, waarbij we aansluiten op de definities gehanteerd in het Cybersecuritybeeld Nederland[14] en het Cybersecurity Woordenboek[15].

1. **Dreiging**: een opzettelijk of niet-opzettelijk gevaar dat kan leiden tot een cyberincident of een combinatie van gelijktijdige of opeenvolgende cyberincidenten.
2. **Risico**: de (combinatie van de) kans dat een dreiging leidt tot een cyberincident én de impact van het cyberincident op belangen, beide in relatie tot het actuele niveau van digitale weerbaarheid.
3. **Cybersecurity**: het geheel aan maatregelen om relevante risico's tot een aanvaardbaar niveau te reduceren. De maatregelen kunnen zijn gericht op het voorkomen van cyberincidenten en – wanneer cyberincidenten zich hebben voorgedaan – deze te ontdekken, schade te beperken en herstel eenvoudiger te maken. Wat een aanvaardbaar niveau is, is de uitkomst van een risicoafweging.
4. **Weerbaarheid**: het vermogen om (relevante) risico's tot een aanvaardbaar niveau te reduceren door middel van een verzameling van maatregelen om cyberincidenten te voorkomen en wanneer cyberincidenten zich hebben voorgedaan deze te ontdekken, schade te beperken en herstel eenvoudiger te maken. Wat een aanvaardbaar niveau van weerbaarheid is, is de uitkomst van een risico-afweging en daarop gebaseerde politieke en/of bestuurlijke keuzen als het gaat om (onder andere) de juiste technische, procedurele of organisatorische maatregelen te kiezen.
5. **Informatiebeveiliging**: Alles wat men doet om ervoor te zorgen dat men bij informatie kan komen wanneer men dat wil, dat de informatie klopt en dat de informatie niet bij anderen terecht komt. Het gaat daarbij vaak om een computersysteem, maar dat hoeft niet. Het gaat om maatregelen, procedures en processen die beveiligingsproblemen voorkomen, opsporen, onderdrukken en oplossen.

14 *Cybersecuritybeeld Nederland 2023* | *Nationaal Coördinator Terrorismebestrijding en Veiligheid (nctv.nl)*

15 *Cybersecurity Woordenboek* | *Cyberveilig Nederland*

Welke dreigingen zijn relevant voor scholen?



Om dit dreigingsbeeld samen te stellen, hebben we gebruikgemaakt van verschillende bronnen, zoals sectorbeelden over het onderwijs en dreigingsbeelden uit andere sectoren, media-berichten over verschillende incidenten binnen het onderwijs en gesprekken die zijn gevoerd in het kader van programma Digitaal Veilig Onderwijs[16]. Om tot een indeling te komen van de dreigingen voor het funderend onderwijs, gebruiken we de relevantste dreigings-categorieën uit het dreigingsbeeld voor het mbo, het hoger onderwijs en onderzoek zoals opgesteld door SURF[17]. Hierbij kijken we bijvoor-beeld naar dreigingen die hebben geleid tot incidenten in het funderend onderwijs, of moge-lijk leiden tot incidenten in de toekomst. Per dreiging leggen we kort uit wat deze inhoudt, geven we praktijkvoorbeelden van incidenten om de dreiging nader te duiden en schetsen we welke maatregelen je als school kunt nemen om je te weren tegen deze dreiging, indien deze relevant is voor de specifieke situatie van de school. Het Normenkader IBP voor het Funderend Onderwijs biedt handvatten voor de maatregelen die genomen moeten worden.

16 *Digitaal Veilig Onderwijs*

17 *Cyberdreigingsbeeld onderwijs en onderzoek 2023 | SURF.nl*

De volgende dreigingscategorieën zijn relevant voor het funderend onderwijs:

- Verkrijging en openbaarmaking van data
- Verstoring van ict
- Overname en misbruik van ict
- Afhankelijkheid van leveranciers en clouddiensten
- Identiteitsfraude en manipulatie van data

Binnen deze dreigingscategorieen hebben we de vijf relevantste dreigingen voor het funderend onderwijs geïdentificeerd:

- Datalekken
- Distributed Denial of Service aanvallen (DDoS-aanvallen)
- Ransomware
- Afhankelijkheid van leveranciers en clouddiensten
- Identiteitsfraude en manipulatie van data

Datalekken

Een relevante dreiging voor scholen is een datalek door een cyberincident zoals malware, phishing, spoofing of hacking, of per ongeluk door handelingen van medewerkers. Bij een datalek raken persoonsgegevens verloren of worden ze ingezien, opgeslagen, aangepast, verzonden of op een andere manier verwerkt door iemand die daar geen recht toe heeft[18].

Verschillende situaties kunnen leiden tot een datalek, zoals:

- Phishing: bij een phishing-aanval proberen cybercriminelen persoonlijke gegevens of wachtwoorden te stelen door je te laten klikken op een link naar een valse website of door je gewoon te vragen deze gegevens te delen. Deze gegevens kunnen dan worden gebruikt om toegang te krijgen tot systemen van de school.
- Spoofing is het misleiden door te doen alsof de crimineel iemand anders is. Bijvoorbeeld door het afzendadres te vervalsen, waardoor het lijkt alsof je met een collega mailt.
- Malware is een verzamelnaam voor ongewenste kwaadaardige software. Een malware-infectie kan ook leiden tot diefstal van persoonsgegevens of verstoorde functionaliteit van systemen binnen de school.
- Ransomware is een specifieke vorm van malware (zie ook dreiging 'Ransomware').

Incidenten

De laatste jaren waren er binnen het funderend onderwijs verschillende incidenten door datalekken. Naast de vervelende gevolgen die een datalek kan hebben voor de personen van wie data gelekt is[19], kan de Autoriteit Persoonsgegevens er een boete voor opleggen.

18 *Wat is een datalek?* | *Autoriteit Persoonsgegevens*

19 *Datalekken: de gevaren en wat moet je doen?* | *Consumentenbond*

Bij een middelbare school in Dordrecht werd door phishing toegang verkregen tot een mailbox, waarna vertrouwelijke gegevens via social media werden gepubliceerd[20]. Op een middelbare school in Drachten werd malware geïnstalleerd door leerlingen, waarna data van leerlingen, ouders en medewerkers online werd gelekt[21]. Op een basisschool voor speciaal onderwijs in Amersfoort werden na een cyberaanval bedrijfsgegevens en verouderde gegevens van medewerkers en cliënten gelekt[22].

Ook kan een datalek impact hebben op de continuïteit van het onderwijs. Zo ontstond er bij een middelbare school in Amersfoort een datalek na een migratie naar een nieuw systeem. Om de omvang van het lek te onderzoeken en het op te lossen, is besloten alle leerlingen naar huis te sturen[23].

Aanbevelingen

Een datalek kan verschillende oorzaken hebben. Om de kans op datalekken te verkleinen, raden wij aan om in ieder geval verschillende basismaatregelen te nemen[24]. Denk hierbij aan het regelmatig installeren van updates om te voorkomen dat kwetsbaarheden misbruikt kunnen worden, en het toepassen van multifactorautenthicatie op de belangrijkste systemen. Daarnaast kun je aan de slag gaan met de voorbeeldmaatregelen uit het Normenkader IBP voor het Funderend Onderwijs uit de domeinen Security Management, Incident en Problem Management en Personeelsbeheer[25]. Als er toch een datalek plaatsvindt, is het belangrijk om de juiste acties te ondernemen, zoals beschreven op de *Aanpak IBP*.

Daarnaast is het belangrijk om te investeren in de bewustwording van medewerkers en leerlingen[26]. Voor specifieke maatregelen tegen phishing verwijzen we je graag naar *de Aanpak IBP* en *de factsheets van het NCSC*.

20 *Hackers zetten privégegevens van medewerkers Dordtse school online (nos.nl)*

21 *Leerlingen scholengemeenschap Liudger hacken laptop docent* | *VPNGids.nl*

22 *Datalek na cyberaanval op Auris Professor Groenschool* | *Nieuws uit de regio Amersfoort (destadamersfoort.nl)*

23 *School dicht door datalek na migratie naar Office* | *Channelweb.nl*

24 *Handreiking Cybersecuritymaatregelen* | *Publicatie* | *Nationaal Cyber Security Centrum (ncsc.nl)*

25 *Normenkader Informatiebeveiliging en Privacy Funderend Onderwijs* | *Aanpak informatiebeveiliging en privacy in het onderwijs (kennisnet.nl)*

26 *Bewustwording* | *Aanpak informatiebeveiliging en privacy in het onderwijs (kennisnet.nl)*

DDoS-aanvallen

Binnen de dreigingscategorieen ‘verstoring van ict’ en ‘overname/misbruik van ict’ is een DDoS-aanval een voor het funderend onderwijs relevante dreiging. Een DDoS-aanval is een aanval waarbij het doel is het systeem onbeschikbaar te maken. Een aanvaller verstuurt zo veel verzoeken dat het systeem het niet meer aan kan, waardoor bijvoorbeeld de internetverbinding uitvalt of een applicatie niet beschikbaar is. Ook kan er van de ict-systemen binnen de omgeving misbruik worden gemaakt om een DDoS-aanval uit te voeren. Binnen het onderwijs wordt veel gebruikgemaakt van onlinediensten. In het geval van een DDoS-aanval zijn deze niet of slecht te gebruiken. Voor een toets of examen bijvoorbeeld, kunnen de gevolgen van een DDoS-aanval groot zijn. Als toetsen digitaal worden afgenomen, en de internetverbinding of het toetsingssysteem is daardoor niet beschikbaar, heeft dit veel impact op leerlingen. Ook een DDoS-aanval op een leverancier kan gevolgen hebben voor leerlingen, bijvoorbeeld als dit plaatsvindt op het leerlingvolgsysteem. Op scholen vinden DDoS-aanvallen vaak door leerlingen zelf plaats. Soms omdat ze bewust het onderwijs of een toets willen verstoren, waarbij ze zich vaak niet realiseren hoe groot de consequenties hiervan kunnen zijn.

Incidenten

Hoewel de dreiging van DDoS-aanvallen op school niet nieuw is, blijft deze actueel. Waar in 2016 al in verschillende media-aandacht werd besteed aan DDoS-aanvallen op scholen[27] zijn er ook incidenten in recentere jaren die het nieuws halen[28]. Het gaat hierbij vaak om aanvallen door leerlingen. Ook andere actoren voeren DDoS-aanvallen uit. Zo is in Nederland het aantal DDoS-aanvallen in het eerste kwartaal van 2023 verdubbeld ten opzichte van het laatste kwartaal van 2022. Hierbij gaat het vooral om geavanceerde aanvallen die gericht zijn op verschillende sectoren in Nederland[29]. Uit statistieken van het Nationaal Dienstencentrum[30] blijkt dat ook in het onderwijs met enige regelmaat DDoS-aanvallen voorkomen, vooral in het voortgezet onderwijs.

Ook leveranciers van het onderwijs kunnen problemen ervaren door DDoS-aanvallen. Zo waren in 2023 de examenuitslagen op verschillende scholen mogelijk vertraagd door een DDoS-aanval op het leerlingvolgsysteem[31].

27 *Hoe DDoS-aanvallen te voorkomen en bestrijden?* | *VO-raad*

28 *Lessen Friese school verstoord na ddos-aanvallen door leerlingen* | *RTL Nieuws*

29 *Opmerkelijke toename van DDoS-aanvallen in het eerste kwartaal van 2023* | *NBIP*

30 *Veilig en betrouwbaar internet voor alle scholen in primair en voortgezet onderwijs bereikbaar*

31 *Examenuitslagen bij twintigtal scholen vertraagd door ddos-aanval* | *Security.NL*

Aanbevelingen

Om de gevolgen van een DDoS-aanval voor je school te beperken, raden wij aan om verschillende maatregelen te nemen, en hier afspraken over te maken met je leveranciers. Daarnaast kunt je aan de slag gaan met de voorbeeldmaatregelen uit het Normenkader IBP voor het Funderend Onderwijs uit de domeinen Security Management en Incident en Problem Management. Voor informatie over specifieke relevante maatregelen verwijzen we je graag naar het DDoS-dossier op de *Aanpak IBP* en de factsheets van het Nationaal Cyber Security Centrum (NCSC) over *DDoS-aanvallen*. Goede internetleveranciers leveren naast diensten als snelheid en betrouwbaarheid ook diensten voor beveiligingsmaatregelen, zoals mitigatie van DDoS-aanvallen en het inrichten van een firewall.

Ransomware

Een andere relevante dreiging binnen de categorie verstoring van ict is ransomware, ook wel bekend als gijzelsoftware. Met ransomware worden systemen geblokkeerd of (persoons)gegevens gegijzeld waarna losgeld wordt gevraagd, zodat het onderwijs stil komt te liggen. Cybercriminelen maken gebruik van een vaak te lage digitale weerbaarheid van slachtoffers, waardoor de potentiële schade van dergelijke aanvallen groot is. Door de schaalbaarheid van ransomware voor cybercriminelen met Ransomware-as-a-Service (RaaS) is de dreiging niet meer alleen gericht op specifieke sectoren, maar meer sectoronafhankelijk geworden[32]. Voor Ransomware-as-a-Service (RaaS) is ransomware-infrastructuur beschikbaar gesteld tegen betaling, waardoor ook criminelen met minder technische kennis een aanval kunnen uitvoeren. Opportuniteit speelt een belangrijke rol: een school die weinig beveiligingsmaatregelen heeft getroffen, is gemakkelijker te hacken. Een voorbeeld hiervan is het in 2021 door de politie offline gehaalde Emotet botnet. Zodra de aanvallers tweefactorauthenticatie aantroffen op een systeem werd de aanval afgeblazen, en gingen de aanvallers door naar het volgende slachtoffer[33].

Incidenten

In de laatste jaren waren incidenten waarbij organisaties getroffen werden door ransomware regelmatig in de media. Voorbeelden hiervan zijn verschillende gemeentes (Gemeente Buren[34], Hof van Twente[35]), maar ook in het onderwijs zijn er incidenten geweest door ransomware. Een middelbare school gaf in 2021 aan door een ransomware-aanval kritieke systemen niet meer te kunnen gebruiken en heeft ervoor gekozen losgeld te betalen[36]. Door de aanval was het onmogelijk om les te geven, zowel online als fysiek.

32 *Cybersecuritybeeld Nederland 2022 | Publicatie | Nationaal Coördinator Terrorismebestrijding en Veiligheid (nctv.nl)*

33 *Cybersecuritybeeld Nederland 2021 | Publicatie | Nationaal Coördinator Terrorismebestrijding en Veiligheid (nctv.nl)*

34 *Gemeente Buren*

35 *Een zwak wachtwoord legde de gemeente Hof van Twente plat | Trouw*

36 *Cyberaanval treft Staring College in Borculo en Lochem: losgeld betaald, school blijft maandag offline | Berkelland | gelderlander.nl*

Ook een scholengemeenschap in Hengelo is slachtoffer geworden van ransomware, waardoor in meerdere scholen de ict-systemen niet beschikbaar waren als gebruikelijk[37].

Niet alleen in Nederland is de dreiging van ransomware relevant voor het onderwijs. In de Verenigde Staten is er een ransomware-groepering actief die zich specifiek richt op K-12 onderwijs (equivalent van het funderend onderwijs in Nederland)[38]. Deze groepering richt zich op het onderwijs vanwege de grote hoeveelheid persoonsgegevens van leerlingen en voert aanvallen vaak uit op cruciale momenten voor scholen, zoals de start van een nieuw schooljaar of de afsluiting van een semester. Bij een schooldistrict in de VS werd hierbij gevoelige data van medewerkers gestolen en gelekt[39]. Deze groep is ook actief in verschillende Europese landen[40, 41].

Aanbevelingen

Om de school te beschermen tegen ransomware kun je verschillende maatregelen nemen.

Als je als schoolorganisatie je eigen ict-omgeving beheert, is het belangrijk om (technische) maatregelen te nemen tegen phishing (zie hiervoor ook de dreiging *Datalekken*, een proces om kwetsbaarheden in systemen te verhelpen in te richten, netwerksegmentering in te richten en verschillende andere technische maatregelen te nemen. Ook goede backups zijn belangrijk om de impact van een eventuele ransomware-aanval te verminderen. Voorbeeldmaatregelen vind je in het Normenkader IBP voor het Funderend Onderwijs in de domeinen Security Management, Incident en Problem Management, IT-operatie en Bedrijfscontinuïteitsmanagement. Voor gedetailleerde maatregelen verwijzen we je graag naar *de Aanpak IBP* en *de factsheets van het NCSC*.

Als het beheer van de ict-omgeving is uitbesteed, is het belangrijk om afspraken te maken met de leverancier over de beveiligingsmaatregelen, hoe je de naleving hiervan kunt controleren en wie welke rol vervult bij een incident. Ook bij uitbesteding blijft de school eindverantwoordelijke. Ook een ransomware-aanval bij een leverancier kan gevolgen hebben voor de continuïteit van het onderwijs of beveiliging van de persoonsgegevens van medewerkers, leerlingen en ouders.

37 *Scholengemeenschap OSG Hengelo getroffen door ransomware-aanval | 1Twente*

38 *#StopRansomware: Vice Society | CISA*

39 *Vice Society claims LAUSD ransomware attack, theft of 500GB of data (bleepingcomputer.com)*

40 *Vice Society ransomware leaks University of Duisburg-Essen's data (bleepingcomputer.com)*

41 *Vice Society claims ransomware attack on Med. University of Innsbruck (bleepingcomputer.com)*

Afhankelijkheid van leveranciers en clouddiensten

Binnen de onderwijssector worden veel Software-as-a-service-oplossingen gebruikt. Dit zijn applicaties of is software die als online dienst wordt aangeschaft en niet zelf worden beheerd.

Ook besteden veel scholen in meer of mindere mate aspecten van hun ict-omgeving uit. Dit biedt voordelen, zoals specifieke kennis bij de leveranciers op het gebied van security, maar brengt ook risico's met zich mee. Scholen hebben, indien er geen goede afspraken zijn met controle op naleving en personeel om dit uit te voeren, beperkt inzicht in de staat van informatiebeveiliging bij hun leveranciers en kunnen ook geraakt worden door de gevolgen van aanvallen die leveranciers raken. Ook als de school niet het primaire doelwit van de aanval is, kunnen er systemen niet beschikbaar zijn door een aanval via de leveranciersketen[42]. Daarnaast bestaat het risico dat leveranciers gegevens van minderjarige leerlingen mogelijk gebruiken voor commerciële doeleinden, als hier geen concrete afspraken over zijn gemaakt of als deze afspraken niet gecontroleerd worden.

Incidenten

Hoewel er op dit moment in het funderend onderwijs geen grote cybersecurity-incidenten bekend zijn als gevolg van de afhankelijkheid van leveranciers, zien we wel verschillende incidenten in andere sectoren. Zo zijn verschillende grote en kleine bedrijven, gemeenten en rijksoverheidsorganisaties geraakt door een datalek bij een softwarebedrijf van een marktonderzoeksbureau[43].

Een ander voorbeeld is een softwarebedrijf dat diensten leverde aan verschillende gemeenten en werd geraakt door ransomware. Daardoor waren bestanden van het administratiesysteem van het sociaal domein versleuteld[44]. Ook de cybersecurity-organisaties van de Verenigde Staten, het Verenigd Koninkrijk, Australië, Canada en Nieuw-Zeeland gaven aan dat er toenemende aandacht is van kwaadwillenden voor *managed serviceproviders* waarbij klanten ook geraakt kunnen worden[45].

Begin december 2021 kwam een kwetsbaarheid in Log4j groot in het nieuws[46]. Deze kwetsbaarheid in een softwarecomponent is illustratief voor het belang van goed inzicht in de afhankelijkheden in de keten en afspraken met leveranciers.

42 *ENISA Threat Landscape 2022 | ENISA (europa.eu)*

43 *Marktonderzoeker Blauw weet nog altijd niet welke data via Nebu is gelekt | Security.nl*

44 *Producten | Informatiebeveiligingsdienst*

45 *Protecting Against Cyber Threats to Managed Service Providers and their Customers | CISA*

46 *Cyberdreigingsbeeld 2021-2022 | Onderwijs en onderzoek (surf.nl)*

Om als school te weten of je kwetsbaar bent, is het niet alleen belangrijk om te weten welke applicaties en software je zelf in huis hebt, maar ook om goede afspraken te hebben met leveranciers over informatievoorziening rondom kwetsbaarheden en updates. Bij een leverancier in het primair onderwijs leidde dit tot een mogelijk datalek, doordat niet met zekerheid was vast te stellen of er persoonsgegevens waren ingezien door gebruik van de Log4j-kwetsbaarheid.

Er zijn daarnaast nog verschillende andere omstandigheden die impact kunnen hebben op de school door de afhankelijkheid in de leverancierskeketen. Wat als de leverancier van digitale leermiddelen en ict-oplossingen niet aan de AVG blijkt te voldoen? Dit kan ervoor zorgen dat per direct bepaalde diensten niet meer te gebruiken zijn in de klas of in de school, hoe belangrijk deze misschien ook zijn voor het onderwijs. Een overhaaste migratie naar een nieuw systeem brengt ook weer beveiligingsrisico's met zich mee, dus is het belangrijk om goed zicht te houden op dit soort risico's in de leverancierskeketen, en tijdig stappen te ondernemen om deze te ondervangen.

Aanbevelingen

Een goed startpunt om deze dreiging te verminderen zijn de afspraken die je maakt met de leverancier. Je kunt bijvoorbeeld aan de slag gaan met de voorbeeldmaatregelen uit het normenkader IBP voor het Funderend Onderwijs uit het domein Ketenbeheer. Maatregelen die leveranciers dienen te nemen om persoonsgegevens op een veilige manier te verwerken zijn beschreven in het Certificeringsschema ROSA[47].

Zo kun je de afspraken over beveiliging van persoonsgegevens opnemen in verwerkersovereenkomsten met leveranciers en gebruikmaken van modelovereenkomsten uit het privacyconvenant[48, 49]. Maar ook als je leverancier geen persoonsgegevens verwerkt. Hiervoor verwijzen wij je graag naar de dienstverlening van SIVON op dit gebied, zoals het collectief uitvoeren van DPIA's en het toetsen van verwerkersovereenkomsten[50].

47 *Certificeringsschema informatiebeveiliging en privacy ROSA | Certificeringsschema informatiebeveiliging en privacy ROSA v3.0 | Edustandaard*

48 *Privacyconvenant onderwijs*

49 *Verwerkersovereenkomsten | Aanpak informatiebeveiliging en privacy in het onderwijs (kennisnet.nl)*

50 *Belangenbehartiging | SIVON*

Identiteitsfraude en manipulatie van data

Een dreiging waarbij de effectiviteit van technische maatregelen duidelijk zichtbaar is, is de dreiging van identiteitsfraude en manipulatie van data. Voorbeelden hiervan zijn leerlingen die toegang proberen te krijgen tot het leerlingvolgsysteem om hun cijfers aan te passen, of het account van de docent proberen over te nemen om geheime informatie te verkrijgen over toetsen. Hiervan zijn vooral voorbeelden bekend in het voortgezet onderwijs. Maar ook in het primair onderwijs is een variatie op deze dreiging actueel, door cyberpesten. Leerlingen kunnen bijvoorbeeld inbreken in het account van een adaptief leersysteem van een medeleerling om met opzet fouten te maken in elkaars opdrachten. De scores van de leerling gaan dan omlaag, terwijl dit niet zomaar hersteld kan worden[51].

Incidenten

In het voorgezet onderwijs waren er enkele jaren geleden verschillende incidenten in de media die te maken hadden met dit onderwerp. Zo fraudeerden leerlingen op een middelbare school in Schiedam met hun cijfers[52], en werden leerlingen op een middelbare school in Amsterdam hier ook bij betrapt[53]. Sindsdien zijn er maatregelen getroffen om deze dreiging tegen te gaan.

Veel leerlingvolgsystemen vereisen inmiddels multifactor-authenticatie voor docenten en beheerders. Ook is er geïnvesteerd in de bewustwording van leerkrachten. En het resultaat mag er zijn: de afgelopen jaren kwamen dergelijke incidenten veel minder voor. Hiermee is de dreiging in theorie nog steeds relevant, maar gelukkig steeds minder actueel.

Aanbevelingen

Zorg ervoor dat belangrijke systemen, zoals het leerlingvolgsysteem, adequaat beveiligd zijn. Het is belangrijk om hier aandacht aan te besteden bij het selecteren van een nieuw systeem of nieuwe leverancier, en dit mee te nemen in de contracten met deze leverancier. Gebruik bijvoorbeeld het *Certificeringsschema informatiebeveiling en privacy ROSA* en *het privacyconvenant* bij de selectie van een leverancier. Ook in het Normenkader IBP voor het Funderend Onderwijs kun je vinden welke maatregelen relevant zijn voor dit soort kritieke systemen. Denk aan het inrichten van toegangsbeleid, gebruik van multifactorauthenticatie, maar ook aan het helpen van gebruikers (zowel onder medewerkers als leerlingen) bij het omgaan met dit soort systemen.

51 *Gepest via Snappet* | *Bureau Jeugd & Media (bureaujeugdenmedia.nl)*

52 *Leerlingen Schiedamse school frauderen met cijfers* | *Rotterdam* | *AD.nl*

53 *Hulp hackende leerling maakt school veiliger* | *De Algemene Onderwijsbond (aob.nl)*

Wat kun je doen tegen deze dreigingen?

Weerbaar zijn tegen cyberdreigingen gaat over risicomanagement: welke risico's zijn er en welke zijn we bereid te accepteren[54]. Het bevoegd gezag moet bepalen welke risicobereidheid er is en of risico's geaccepteerd kunnen worden of gemitigeerd moeten worden. Het Normenkader IBP voor het Funderend Onderwijs beschrijft verschillende normen voor het inrichten van risicomanagement, het uitvoeren van risicoanalyses en het koppelen van risico's aan beheersmaatregelen. Dit dreigingsbeeld kun je gebruiken als input voor risicomanagement en de risicoanalyses die je zelf uitvoert. Welke dreigingen zijn voor jou het meest relevant en voor welke systemen of processen zijn ze dan het meest relevant? Als bepaalde processen of systemen zijn uitbesteed, is het ook belangrijk om je leverancier te bevragen op de genomen maatregelen tegen de dreigingen die voor jouw school relevant zijn.

In het programma Digitaal Veilig Onderwijs wordt in 2023 ook een sectorale risicoanalyse uitgevoerd. Deze risicoanalyse kan als startpunt dienen voor het gesprek over de risico's binnen jouw school. Om risicomanagement te borgen binnen de organisatie, is het belangrijk dat risico's niet alleen worden besproken binnen de ict-afdeling of door de bij dit onderwerp betrokken medewerkers, maar ook met andere medewerkers en op het niveau van de bestuurder. Hiermee kun je specifieke maatregelen inrichten, waarmee je de risico's kunt adresseren, en invulling geeft aan de normen in het Normenkader IBP voor het Funderend Onderwijs.

54 *Programmaplan | Digitaal Veilig Onderwijs (DVO) 2023*

Colofon

Dreigingsbeeld Funderend Onderwijs

Datum van uitgave
September 2023

Auteurs
José Teuwen

Eindredactie
Nanda van Dijk

Vormgeving
Delta3, Den Haag

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).

Bit by Bit
Samen voor digitaal veilig onderwijs

kennisnet.nl

Kennisnet
Postbus 778
2700 AT Zoetermeer

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