Terugkoppeling rondetafelbijeenkomst cyberveiligheid in het onderwijs, 11 oktober en 10 november 2022

Elke onderwijsinstelling in het primair onderwijs, voortgezet onderwijs, speciaal onderwijs, middelbaar beroepsonderwijs en hoger onderwijs werkt met digitale systemen en kan te maken krijgen met risico's rond cyberveiligheid. Als bestuurder bent u verantwoordelijk voor de continuïteit van het onderwijs en de beveiliging van persoonsgegevens van leerlingen, studenten, medewerkers en andere betrokkenen. Eerder had de Inspectie van het Onderwijs contact met onderwijsinstellingen naar aanleiding van incidenten en verscheen in 2021 een themaonderzoek naar de cyberweerbaarheid in het hoger onderwijs. In juli 2022 stuurden de ministers Wiersma en Dijkgraaf een brief naar de Kamer met daarin de aanpak om te komen tot het verhogen van de digitale veiligheid in het onderwijs en onderzoek. Naar aanleiding van de toenemende aandacht en belang voor cyberveiligheid organiseerde de Inspectie van het Onderwijs in het najaar van 2022 voor bestuurders uit het hele onderwijsveld twee rondetafelbijeenkomsten over cyberveiligheid.

Leren van elkaars ervaringen
Het doel van deze bijeenkomsten was het leren van elkaar: Wat betekent cyberveiligheid voor uw instelling? Welke uitdagingen komen op uw scholen en opleidingen af? Iedereen gebruikt verschillende digitale systemen en kan te maken krijgen met de keerzijde hiervan. Het maakt niet uit of u een grote onderwijsinstelling bent of een zelfstandige school (eenpitter) en binnen welke sector u actief bent, iedereen was welkom. Door praktijkervaringen uit te wisselen en dilemma's te bespreken konden bestuurders nadenken over de weerbaarheid van de eigen instelling. Ook was de inspectie nieuwsgiering naar wat er binnen besturen, scholen en opleidingen leeft op het gebied van cyberveiligheid.

Deelname
De twee bijeenkomsten brachten een zeer divers gezelschap bij elkaar. We ontmoetten elkaar van basisscholen tot universiteiten, zowel grote als hele kleine onderwijsorganisaties en zowel uit het bekostigd als het niet-bekostigd onderwijs. De deelnemers zijn werkzaam in allerlei verschillende functies, waaronder die van bestuurder, Functionaris Gegevensbescherming (FG), IT'er, beleidsmaker en inspectiemedewerker.

Wat leest u verder in dit verslag?
Dit document doet verslag van de bijeenkomsten op 11 oktober 2022 in Zwolle en 10 november 2022 in Den Bosch. Het betreft een geïntegreerd verslag van beide bijeenkomsten en de gesprekken die daar zijn gevoerd. Het verslag bevat tevens handouts van de presentaties die tijdens de bijeenkomsten zijn getoond.

Inhoudsopgave

Plenaire start: Hoe werken hackers?

De bijeenkomst werd afgetrapt met een presentatie door **Mark Koek**, oprichter en directeur van HackDefense. Hij nam iedereen mee in de werkwijze van hackers en wees ons daarbij op de uitdagingen voor bestuurders en IT'ers. De handout van de presentatie is opgenomen vanaf pagina 29.
Met de presentatie wil Mark de mystiek rond hackers wegnemen. Zo zijn hackers geen tovenaars maar gewone mensen. En helaas, een hack 100% voorkomen is onmogelijk maar het probleem is hanteerbaar, we kunnen er dus iets aan doen. Ga aan de slag met preventieve maatregelen, bewustzijn in de hele organisatie en zorg voor een getrainde calamiteitenorganisatie.

Onderwijs als object van aanval

- Onderwijsinstellingen maken net als andere organisaties en individuen gebruik van veel IT-systemen die met het internet verbonden zijn. Systemen die het onderwijs gebruikt zijn niet wezenlijk anders dan organisaties in het bedrijfsleven gebruiken.
- Het onderwijs kenmerkt zich door een zeer diverse gebruikersgroep met daarin medewerkers, leerlingen, studenten en ouders. Met veel verschillende leerlingen en/of studenten is het onderscheid tussen de "buitenkant" en de "binnenkant" meer diffuus dan elders. Bedreigingen komen niet alleen van buiten, maar ook van binnenuit. Leerlingen en studenten kunnen bijvoorbeeld moedwillig, maar ook onopzettelijk systemen platleggen.
- Actueel voorbeeld: een leerling bestelt 10.000 licenties via het schoolsysteem ter waarde van €500.000. Hierbij is er eigenlijk geen hack gepleegd, het bleek binnen het systeem simpel mogelijk voor een leerling dit te doen. Deze ''bestelling'' werd gelukkig opgemerkt door de leverancier die bij de onderwijsinstelling verifieerde of de bestelling wel klopte. Hier zat de kwetsbaarheid dus in de procedure en de controle op de rechten.
- Het huidige verdienmodel door dreigingen van buiten de organisatie is ransomware. Dit is niet gericht op een specifieke organisatie of sector. Er wordt gewoon willekeurig heel veel gehackt en als hackers een kwetsbaar netwerk aantreffen dan zullen ze die kans aangrijpen. Het onderwijs kan dus ook slachtoffer worden van cyberaanvallen. Dat is met verschillende aanvallen op onderwijsinstellingen in alle sectoren, po, vo, so, mbo en ho, al bewezen.

Aanvallers

- Zelden is het één persoon of groep waar je door wordt aangevallen. Er zijn groepen gespecialiseerd in het uitvoeren van één van de stappen van een aanval (ontfutselen wachtwoorden, afpersen etc).
- Cybercriminelen werken in ketens samen. Het is een businessmodel. Losgeld betalen betekent veelal dan ook dat je de sleutel krijgt om je bestanden te kunnen ontsleutelen en door de hackers wordt hierbij vaak ook hulp aangeboden.
- Cybercriminelen innoveren: ze ontwikkelen nieuwe tools om succesvoller aan te vallen. Met beveiligen van het onderwijs ben je dus nooit klaar.
- Wat in de publiciteit komt is het topje van de ijsberg.

Hoe werkt hacking (voorbeeld ransomware)?

- Eerst inbraak in account van een medewerker, leerling of student. Hoe? Door het wachtwoord te raden. Mensen zijn niet goed in het bedenken van sterke wachtwoorden en gaan dat ook nooit worden. Een *passwordmanager* kan helpen gebruik van hetzelfde paswoord bij verschillende applicaties en websites tegen te gaan. Wat echt helpt is *Multifactor-authenticatie* (is een must). Dit betekent dat je naast inloggen met een wachtwoord nog een ander middel nodig hebt, bijvoorbeeld een gegenereerde code.
  Of de eerste inbraak gaat via phishing. Slachtoffer klikt op een malafide link en logt in waardoor het wachtwoord kenbaar wordt gemaakt aan de hacker. *Periodiek phishing-testmails* rondsturen helpt. Mensen leren ervan als je zorgt dat ze na het klikken uitleg krijgen over hoe ze de phishingmail hadden kunnen herkennen. Maar 100% voorkomen lukt nooit. Daarnaast is het belangrijk dat iedereen weet waar zij in de organisatie phisingmails kunnen melden. Als mensen snel melden dan heb je tijd om te repareren. Wees positief naar melders, straf ze niet af, maar stimuleer het melden.
- Escalatie: de hacker heeft toegang tot één account en gaat op zoek naar alle gegevens op het netwerk. Hoe? Hacker probeert toegang te krijgen tot een account met meer rechten, zoals een netwerkbeheerder. Er is altijd wel ergens achterstallig onderhoud, een update vergeten of een oude server waar meerdere mensen rechten op hebben. Zorg voor tijdig *onderhoud*, voer een *grote schoonmaak* uit (voor de zomervakantie bijvoorbeeld) en heb aandacht voor het in kaart brengen van alle IT in de organisatie; zijn er ook vergeten of verouderde systemen?
- Exfiltratie (niet altijd): alle data downloaden die de hacker kan vinden. De hacker kan dreigen om deze gegevens openbaar te maken. Er kan gekozen worden om de stap niet of niet volledig uit te voeren. Omdat deze stap tijd kost kun je als hacker ontdekt worden. Grotere bedrijven/instellingen *monitoren* of er grote hoeveelheden data gedownload worden.
- Back-ups vernielen: een hacker gooit alle back-ups weg. Het slachtoffer wordt dus afhankelijk van de hacker om zijn informatie terug te krijgen.
  Zorg voor *back-ups ook los van het netwerk*
- Encryptie toepassen: dit gebeurt door versleuteling. Met de juiste sleutel kan dit ongedaan gemaakt worden. Je hebt dus óf de back-up nodig óf de sleutel die de hacker heeft. De sleutel is tegen betaling bij de hacker verkrijgbaar, waarbij wordt gedreigd data openbaar te maken (afpersing).
- Hackers krijgen toegang tot willekeurige accounts en bestanden met login-gegevens worden te koop aangeboden op het darkweb.
- Soms zit er veel tijd tussen de eerste stap en de tweede.
- Niet alle stappen worden altijd volledig doorlopen.

Verantwoordelijkheden

- Cyberveiligheid is een hanteerbaar probleem, maar niet alleen de verantwoordelijkheid van de IT afdeling. Ga aan de slag in de onderwijsinstelling met preventieve maatregelen, bewustwording en een aanpak om calamiteiten te bestrijden.
- Verantwoordelijkheid ligt óók bij het bestuur. Mensen die verantwoordelijk zijn moeten ook de bijbehorende bevoegdheden hebben. Het beveiligingsbeleid moet niet bij IT liggen.

- Er moet genoeg budget zijn voor IT. Ook genoeg tijd en personeel is van belang. Blije IT'ers die de tijd hebben om het IT-landschap in kaart te brengen en de benodigde expertise hebben, vormen een onderdeel van je verdediging.
- IT is niet voor erbij, maar een wezenlijk bedrijfsproces.
- Voorkom dat het een papieren exercitie wordt.
- Zorg voor voldoende tijd om de basishygiëne op orde te houden.
- Wees voorbereid op calamiteiten. Uit de zaal werd gevraagd:
    - *Is een verzekering nuttig voor cyberrisico's?*
      Kan nuttig zijn mits verzekeraars bepaalde eisen stellen aan de professionaliteit van het IT-beveiligingsbeleid en hieraan wordt voldaan. Dit is nog erg in ontwikkeling en kan zelfs de door hackers geëiste bedragen verhogen.
- Er is altijd mensenwerk nodig, omdat software de context die voor jouw onderwijsinstelling geldt niet snapt. Zo kwamen vanuit de zaal vragen over het inzetten van Multifactor-authenticatie (MFA):
    - *MFA is leuk maar hoe werkt dat bij jonge leerlingen?*
      Klopt, het kan niet altijd maar dan moet door het bestuur een keuze gemaakt worden en eventuele andere mitigerende maatregelen worden ingevoerd.
      Er kan worden gekozen om MFA alleen bij externe toegang toe te passen, en intern niet. Dit levert wel een klein extra risico op.
    - *Moeten wachtwoorden periodiek worden aangepast?*
      Bij Multifactor-authenticatie (MFA) niet meer persé nodig, kun je bijvoorbeeld als "wisselgeld" inzetten bij de invoering van MFA.

Sessie 1. Hoe cyberweerbaar is mijn onderwijsinstelling?

Met medewerking van:
Larissa Zegveld – voorzitter forum standaardisatie en directeur-bestuurder van Kennisnet
Pieter Rogaar –Adviseur cybersecurity bij Kennisnet
Chris Zintel - programmamanager Veilig digitaal funderend onderwijs bij Kennisnet
Brenno de Winter – Chief Security en Privacy Operations bij het Ministerie van Volksgezondheid, Welzijn en Sport, directie Informatiebeleid, programma Realisatie Digitale Ondersteuning.
Bij deze sessie werd een inleiding gegeven door Kennisnet in samenwerking met Brenno de Winter. De handout van de presentatie is opgenomen vanaf pagina 35.

Cyberweerbaarheid is een keuze

Inleiding Brenno de Winter over OpenKAT

- Kennisnet krijgt van bestuurders vaak de opmerking 'Ik ben maar een kleine school, ik heb niet zoveel interessante gegevens, dus ik word niet gehackt'. We hebben in de presentatie van Mark Koek ook al gehoord dat hackers zich niet laten leiden door schaalgrootte en sector. Brenno en Larissa hebben er samen een podcast over gemaakt: Cybersecurity in het onderwijs - een gesprek met Brenno de Winter (kennisnet.nl)
- 100% veilig bestaat niet, hackers ontwikkelen immers ook door. Hoe weet je als bestuurder dat de activiteiten die je ontplooit de juiste zijn? Kwetsbaar is een breed begrip. Wat voor jou kwetsbaar is, hoeft dat voor een andere instelling niet te zijn. Weerbaar betekent ook je bewust zijn van je kwetsbaarheid en een plan hebben voor het geval dat.
- Tijdens de corona-lockdown in 2020 bleek dat voor cyberveiligheid nog veel aandacht nodig was en dat het zorgde voor hoge werkdruk. Bij het Ministerie van Volksgezondheid, Welzijn en Sport (VWS) werd erover nagedacht hoe dit anders zou kunnen en werd OpenKAT bedacht. KAT staat voor Kwetsbaarheden Analyse Tool. Deze tool is recent opgenomen in het actieplan Nederlandse Cybersecuritystrategie 2022-2023.[1] Het idee is: door kwetsbaarheid te omarmen kan er beter nagedacht worden over de vraag wat maakt ons kwetsbaar? Voldoet een site aan de normen die relevant zijn voor veiligheid?
- Wat maakt een site kwetsbaar?
  - Technische problemen
  - Niet voldoen aan de standaarden (non-compliance)
  - Onveilige praktijken
  - Veranderingen in omgevingen
- In securityland wordt een lek opgelost zodra die zich voordoet. KAT verzamelt continu alle feiten (forensisch geborgd) zodat je bij een lek direct kunt zien waar in het systeem het lek zit en je het probleem zo snel kunt oplossen. KAT verzamelt feiten door ze te sorteren. Als je zoekt naar een speld in een hooiberg, heeft KAT al hooi bij hooi en spelden bij spelden gesorteerd. KAT zoekt niet, maar je vult zelf de database met de

[1] Zie: https://www.rijksoverheid.nl/documenten/publicaties/2022/10/10/actieplan-nederlandse-cybersecuritystrategie-2022---2023

relevante opgezochte feiten. Alles wat je ooit hebt opgezocht, blijft opgeslagen in de database.

- Standaarden zijn de oplossing. KAT helpt je hierbij door deze standaarden voor je op te slaan. Als er iets in de database verandert krijg je een waarschuwing. Voldoe je nog aan de standaarden? Zo niet, is dit een probleem? Als we ons meer houden aan de standaarden, draagt dit bij aan veiligheid.
- Bij jaarlijkse audits wordt teruggekeken. Pentests zijn een momentopname; een lijst met bewijs van stukken die op dat moment *niet voldoen.* Het is wenselijk als het rapport meer lijkt op de APK voor auto's: deze punten zijn gecheckt en dat klopt wel en dat klopt niet. Door KAT is dit geautomatiseerd, het rapport is veel meer up-to-date omdat er op meerdere momenten bekeken wordt hoe het ervoor staat, niet slechts één keer per jaar. Auditors willen graag weten: opzet – bestaan – werking en met KAT is dit mogelijk.
  KAT is een cross-time database; je kunt terug in de tijd waardoor je ook achteraf de historie kunt bekijken. Je kunt dus bewijzen dat je het hele jaar compliant bent geweest en dat de cyberveiligheid technisch was geborgd 1 minuut voordat alles plat ging. Door KAT heb je ook meer zekerheid dat je de juiste processen hebt ingeregeld en dat je dit kunt aantonen. De inrichting van dit proces geeft de bestuurder houvast.
- OpenKAT is nu een jaar in gebruik en is voor iedereen beschikbaar via de website https://openkat.nl/ (open source). VWS-medewerkers hebben eerst de techniek ontwikkeld en zijn nu volop aan het testen. Daarbij hebben ze ook andere sectoren nodig dan VWS. Ze werken samen met Z-CERT die in de zorg een proef gaat doen met OpenKAT. Ook het NCSC is aan het kijken of KAT een oplossing is voor hun organisatie. Kennisnet test OpenKAT nu intern en gaat met het KAT-team kijken of ze het voor de onderwijssector toepasbaar kan maken. Iedere instelling die nu al wil meedoen, kan dat doen via de eerdergenoemde website.
- Er worden met de Open Community dagen georganiseerd over de standaarden. Het is aan te raden om hierbij aan te haken, omdat dit helpt om KAT eerder beschikbaar te hebben voor het onderwijs.
- Kleine instellingen maken vaak gebruik van outsourcing. Het rapport dat gegenereerd wordt door KAT gaat naar de bestuurder en de outsourcepartij (de leverancier), zodat beiden weten van welke kwetsbaarheden er sprake is.

Het funderend onderwijs is onvoldoende digitaal veilig

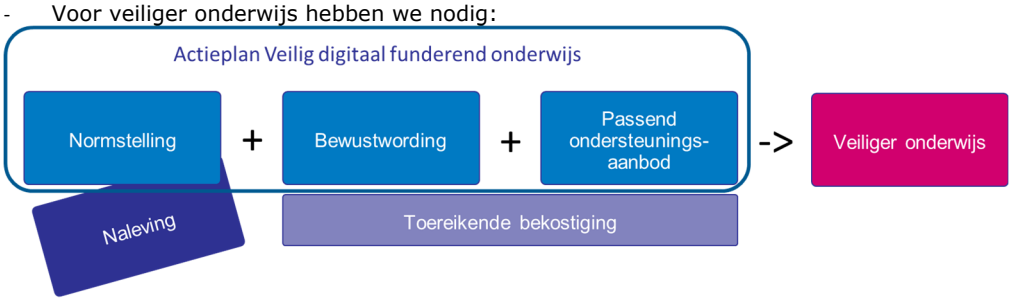
Hoe kan Kennisnet het funderend onderwijs ondersteunen in het proces van digitaal veiliger worden? Een gecoördineerde aanpak is gewenst.

Probleemanalyse

- *Wat:* het is voor schoolbesturen onvoldoende duidelijk wat 'veilig' inhoudt en wat daarvoor gedaan moet worden.
- *Wie:* de consequenties van het niet goed regelen van privacy en beveiliging worden door schoolbesturen onvoldoende gevoeld.
- *Hoe:* het is voor individuele schoolbesturen zeer kostbaar en in sommige gevallen moeilijk uitvoerbaar om alle passende maatregelen op het gebied van privacy en cybersecurity te organiseren.

- Er moeten landelijke normen komen om te bepalen wat 'veilig' is. PO-Raad/VO-raad, OCW en SIVON zijn met de onderwijspartijen in gesprek gegaan t.b.v. veilig digitaal onderwijs voor alle leerlingen in het funderend onderwijs. Hiermee hebben ze de handschoen van Dennis Wiersma opgepakt om de digitale veiligheid onderwijs en onderzoek te verbeteren, zoals opgeroepen is in de kamerbrief van 14 juli. Het is belangrijk om een gedeeld beeld te hebben van wat er aan de hand is (probleemanalyse).

- Voor veiliger onderwijs hebben we nodig:



Wat moet ik doen? = normstelling,
Waarom moet ik het doen?: er wordt geïnvesteerd in bewustwording
Hoe moet ik het doen?: passend ondersteuningsaanbod geeft veiliger onderwijs

1. De wet Naleving Normstelling

- Er wordt gewerkt aan een normenkader met daarin de eisen waaraan instellingen moeten voldoen; dat gaat lijken op hoe het in het hoger onderwijs gaat. Voor de toepassing wordt gekeken of de normen ook passend en toepasbaar zijn voor het funderend onderwijs. Het uiteindelijke doel is één wettelijk kader voor het gehele onderwijsveld.
- Kennisnet richt zich op (cyberveiligheid) in het funderend onderwijs. SURF richt zich op het bekostigde hoger onderwijs en het middelbaar beroepsonderwijs. Kennisnet vormt op dit moment geen alliantie met SURF, omdat SURF en het hoger onderwijs al "volwassener" zijn op het gebied van cyberveiligheid. SURF heeft een andere mate van volwassenheid en er is een ander CERT nodig voor het funderend onderwijs dan SURF-CERT. SURF levert bouwstenen, Kennisnet moet dienstverlening leveren. SURF heeft een lidmaatschapsmodel waarbij onderwijsinstellingen 0.2 fte uitlenen aan deze centrale CERT.
- Het normenkader wordt in de eerste helft 2023 openbaar en wordt uiteindelijk wettelijk verplicht. Wegens de vrijheid van het onderwijs kun je enkel per wet deze vrijheid beperken. Aan wetgeving zit altijd een implementatietermijn vast, omdat niet iedere instelling direct aan bepaalde normen kan voldoen. Er komt een Actieplan voor veilig digitaal funderend onderwijs. Het is de bedoeling om dit samen te doen, niet iedere instelling voor zich.
- Normenkader en wetgeving moeten duidelijk gaan maken hoe naleving wordt vormgegeven en wat de rol van de inspectie en/of Autoriteit Persoonsgegevens is. Het moet duidelijk zijn aan wie instellingen zich moeten verantwoorden. Aan het normenkader zit een toetsingskader vast om te zorgen dat zaken uniform uitgevraagd

worden. Het doel van een normenkader en bijbehorende wetgeving is om het volwassenheidsniveau op cybersecurity van de onderwijssector te verhogen.
- Het hoger onderwijs streeft er naar niveau 3 te halen. Nu is dat een papieren werkelijkheid die we in de praktijk moeten testen. Veel instellingen hebben nu beveiliging als een kokosnoot: de firewall is hard, maar als je daar doorheen bent is het zacht. We willen naar een ui: diverse schillen zodat elk deel apart beveiligd is.

2. Bewustwording is vooral de verantwoordelijkheid van de bestuurder.
- Bestuurders moeten zorgen dat het onderwerp aandacht krijgt binnen de gehele organisatie. Bestuurders zullen maatregelen moeten nemen met als doel cyberveiligheid goed ingeregeld te hebben. De verbinding tussen de bestuurder en ICT-medewerkers moet vaak nog gemaakt worden. ICT-medewerkers voelen zich nog snel aangevallen door vragen van het bestuur, terwijl het oprechte vragen zijn. In die cultuur kunnen nog stappen gemaakt worden. Dit onderwerp komt op de eerstvolgende ALV's (november 2022) van de PO-Raad/VO-raad op de agenda.
- Het is best lastig om 800 medewerkers mee te nemen in verandering en bewust te maken van het belang van cyberveiligheid; iedereen wil onderwijs maken en dan moet dit ook nog! Het is daarom raadzaam om het laagdrempelig aan te bieden en geleidelijk op te schalen zodat besturen dit zelf kunnen vertalen naar hun instelling. Begin bij bewustwording van besturen en rectoren bijvoorbeeld door cyberveiligheid op te nemen in het inwerkprogramma.

3. Passend ondersteuningsaanbod: zoveel mogelijk samen doen en centraal beleggen.
- Bij ondersteuningsaanbod hoort ook een toereikende bekostiging: elk jaar 6M euro. Veel partijen geven nu al aan dat dit bedrag veel te laag is.

OpenKAT valt voor een deel in 1) normstelling/naleving en in 3) passend ondersteuningsaanbod.

Reacties en vragen uit de zaal
Deelnemers herkennen de bijdrage van Kennisnet:
- Zo spreekt een deelnemende bestuurder uit weinig collega bestuurders te zien. Er is geen bewustzijn, landt niet, er is geen voedingsbodem. Goed initiatief van de inspectie!
- Bestuurders moeten in beweging komen.
- Herken me in de analyse; experts gaan voor een 10. Maar dat is alle dagen niet werkbaar. Welke keuzes maak je dan?
- Een bestuurder geeft aan: Normenkader zorgt voor bewustwording! Ons digitaal register wordt gescreend. Heel handig om te weten waar je op moet controleren.
- Larissa Zegveld deelt eerdere ervaring: Toen we dit bij de hand hadden bij de VNG waren er burgemeesters die als ambassadeur langs gingen bij andere burgemeesters.
- Brenno de Winter: we denken cultureel niet vanuit veiligheid in NL.

Mag je beschikbaarheid van continue kwetsbaarheid-informatie (zoals KAT levert) ook verwachten van de derde partij waar je hebt gehost?
Nog niet, maar de jurisprudentie gaat wel die kant op. In de rechtspraak is nu de beheerder verantwoordelijk ook al heeft hij gewaarschuwd. Gewaarschuwd maar geen gehoor, dan kun je als beheerpartij de portefeuille teruggeven.

Supplychain met digitaal verwerkingsovereenkomst: Klopt wat wij afspreken met leveranciers en de serviceorganisatie?
SIVON en Kennisnet zijn bezig om te controleren of het klopt en hebben hiervoor contact met Magister en ParnasSys. (zie ook sessies 3 en 4)

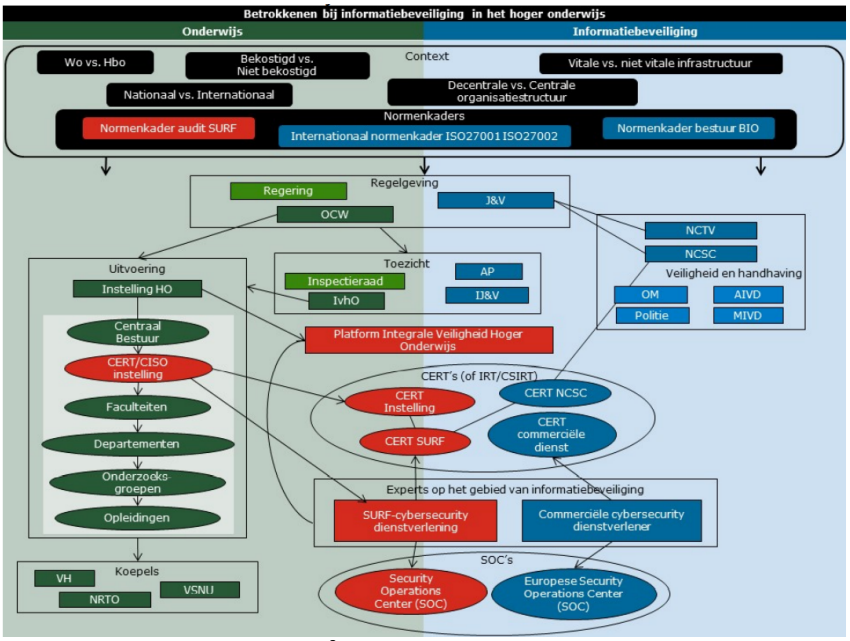
Assetmanagement: zicht op leermiddelen
In sessie 3 kwam aan de orde dat scholen vaak geen idee hebben welke digitale leermiddelen docenten inzetten waarin bijvoorbeeld persoonsgegevens voorkomen. Dat kunnen we niet uitbannen. Maar waar stuur je op als bestuurder? Docenten beroepen zich op hun autonomie. Als je het al in beeld hebt, wat doe je er dan mee?
Reactie Kennisnet: als bestuurder wil je inzicht in data en processen. Bij nieuwe applicaties kun je docenten verplichten eerst bij de CISO te vragen of er een controle kan plaatsvinden om te zien of er al een overeenkomst is met de aanbieder. CISO bepaalt dan of een applicatie gebruikt kan worden.

Sessie 2: Wie is verantwoordelijk voor veilig digitaal onderwijs?

De vraag die in deze workshop centraal stond was: wie is verantwoordelijk? Die vraag kun je op verschillende niveaus beantwoorden. In deze workshop hebben we met elkaar gesproken over wat verantwoordelijk eigenlijk betekent.

Samenvattend

- Er zijn al veel mooie initiatieven, maar die zijn nog lang niet overal bekend. Dat vraagt ook verantwoordelijkheid nemen; juist bestuurders die zich bewust zijn van risico's, zijn beter voorbereid en zoeken zelf actief naar informatie. Deze gesprekken voorzien in een behoefte om met elkaar ervaringen en zorgen te delen, zonder hier direct op te worden afgerekend.
- De verantwoordelijkheid werkt ook andersom: het bereiken en betrekken van de groep die zich minder bewust is en minder goed is toegerust. Er zijn wel diverse initiatieven vanuit koepels, OCW en ook regionaal voor samenwerking en kennisdeling.
- Er is behoefte aan duidelijke kaders die niet mogen knellen en die ook aangeven wie waar over gaat. Er moet ruimte blijven voor verschil in ontwikkelsnelheid en volwassenheidsniveau. Daarbij moet de ondergrens wel duidelijk zijn en er moet hulp zijn voor achterblijvers.
- Scholen hebben behoefte aan voldoende middelen om hun verantwoordelijkheid ook goed in te kunnen vullen. Dat betekent niet alleen geld, maar ook loketten met kennis en kunde, professionaliseringsaanbod, ruimte voor oefening.



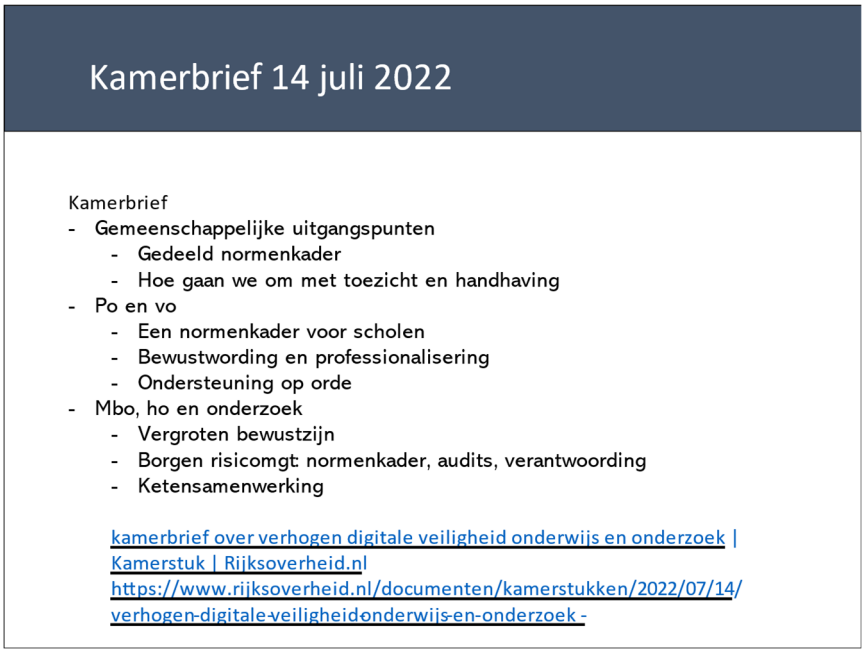
Dia 1 Overzicht stelsel cyber-onderwijs HO[2]

[2] Bron: https://www.onderwijsinspectie.nl/onderwerpen/cyberveiligheid/documenten/themarapporten/2021/09/15/digitale-weerbaarheid-in-het-hoger-onderwijs

De kaart van verantwoordelijkheden in Nederland

- We zien twee werelden: onderwijs en cyber. Ter illustratie de verschillende actoren in het hoger onderwijs (figuur 1). Voor andere sectoren kun je vergelijkbare plaatjes maken. Bij cyberveiligheid ontmoeten die twee werelden elkaar, terwijl ze elkaar eigenlijk niet goed kennen. Dat betekent dat we aan de slag moeten. We hebben wel hetzelfde doel: weerbaarheid verhogen. Dat kan alleen als je weet wat ieders rol is en wie aan welke knoppen draait.
- 'Het onderwijs' bestaat niet, we zien grote verschillen tussen onderwijsinstellingen:
  - van enkele leerlingen tot 40.000 deelnemers, van 1 opleiding tot 100+ opleidingen
  - Van 1 locatie tot internationaal
  - Fase van ontwikkeling, volwassenheidsniveau, weerbaarheidsniveau
- Instellingen hebben ook te maken met verschillende wettelijke kaders.
- Het helpt om voor jezelf te bedenken: hoe ziet die kaart er voor mijn eigen instelling uit? Hoe ziet mijn omgeving er uit? Met wie moet ik afstemmen?

Het Ministerie van OCW licht in de sessie de kamerbrief[3] toe die in juli is verstuurd: naast een gezamenlijk normenkader, ook specifieke maatregelen voor funderend en niet-funderend onderwijs.



Dia 2 Hoofdpunten kamerbrief 14 juli

[3] https://www.rijksoverheid.nl/documenten/kamerstukken/2022/07/14/verhogen-digitale-veiligheid-onderwijs-en-onderzoek

Wat is je eigen rol en verantwoordelijkheid als bestuur

- Tijd is belangrijk: er zijn veel prioriteiten die op een school afkomen. Zeker een kleinere school kan niet alles tegelijk. Het is niet zo dat digitalisering in het onderwijs belangrijker is dan andere bedrijfsvoeringstaken. Wel is er een duidelijke link met de continuïteit van het onderwijs. Daarom van groot belang, maar niet altijd direct tastbaar: het is een bedreiging in de toekomst die strijdt met belangen in het hier en nu.
- Je zult ook meer moeten samenwerken, je kunt niet wachten tot je tijd hebt. In sommige regio's gebeurt dit al. Hierbij kun je leren van elkaar en kun je al quick wins zien en kijken naar good practices. Er is een groot schoolbestuur dat kleine besturen uit de regio de mogelijkheid biedt om voor een beperkt bedrag aan te sluiten bij hun ICT.
- Eerste stap is bewustwording. Een kleine hack kan enorm helpen bij het vergroten van het bewustzijn. ICT'ers vinden het moeilijk om cyber bij de bestuurder op de agenda te krijgen. ICT'ers zien de risico's wel, maar krijgen weinig gehoor.
- Cyberveiligheid is onderdeel van het risicomanagementsysteem. Want stel dat je IT-systemen morgen plat liggen, wat dan? Wie ga je bellen? Wat staat klaar? Staat er een incident respons team klaar? Cybersecurity zou onderdeel moeten zijn van het veiligheidsplan van een school.
- Belangrijk is om de juiste trigger te vinden om beweging te creëren. Dat kan bijvoorbeeld innovatie zijn. Maar in het onderwijs wordt 'out of the box' denken vaak eng gevonden.
- Cybersecurity wordt nu nog vaak weg gedelegeerd. Scholen worden zich wel steeds meer bewust van hun beleidsverantwoordelijkheid. Bestuurders zouden graag willen weten: wie zijn de autoriteiten en wie heeft welke kennis in huis? Als bestuurder hoef je niet overal verstand van te hebben. Je hoeft het zelf niet te weten/kennen/kunnen, maar je moet er wel begrip voor hebben. Je moet de juiste vragen kunnen stellen. Bij outsourcing moet je altijd doorvragen op veiligheid. Hulp over welke vragen je hierbij moet stellen is wel nodig.

Bekwaamheid oefenen

- Voor digitalisering is professionalisering nodig. Is er professionaliseringsaanbod voor bestuurders? Op bestuursniveau is er onvoldoende kennis/kunde rond cyberveiligheid. Het normenkader gaat zeker helpen, want daar wordt een bestuurder op aangesproken.
- Een bestuurder heeft een mooie oplossing: 'train de trainer'. Aan het eind van de dag zijn dan 350 mensen een stuk bekwamer. Thema: door te delen wordt het meer.
  Op zijn vo-school wordt elk jaar een hackers-dag gehouden. Leerlingen zagen op zo'n dag kans om Magister te hacken. Vervolgens hebben ze Magister uitgenodigd, zodat ze konden uitwisselen hoe ze dat gedaan hebben en hoe Magister zoiets een volgende keer kan voorkomen.
- Tip: doe een oefening. Laat iedereen zijn telefoon inleveren en zeg: alles ligt plat, wat gaan we nu doen? Zo kun je het mooi opbouwen: wie bel je eerst, wie is de volgende?
  In SURF-verband worden OZON-oefeningen gehouden. Daarbij pakken ze iets actueels, iedereen kan meedoen. Is goed om een crisisteam heel strak samen te stellen. Zorg dat je het plan voor een crisis op papier hebt staan (want je kunt niet meer in je systemen).
  Het zou goed zijn als elke schoolbestuur regelmatig een oefening met een crisissituatie zou doen, zoals ook een brandoefening wordt gehouden. Dit kost wel tijd en geld. Maar: Kun je je wel voorbereiden op elke crisis? En is dat het wel waard?

- Er zijn al zo veel goede voorbeelden, er is genoeg om van te leren. Ga het wiel niet zelf uitvinden maar kijk bij de buren en kijk over de muren van de onderwijssectoren heen.

Normstelling door de overheid of zelfregulering?

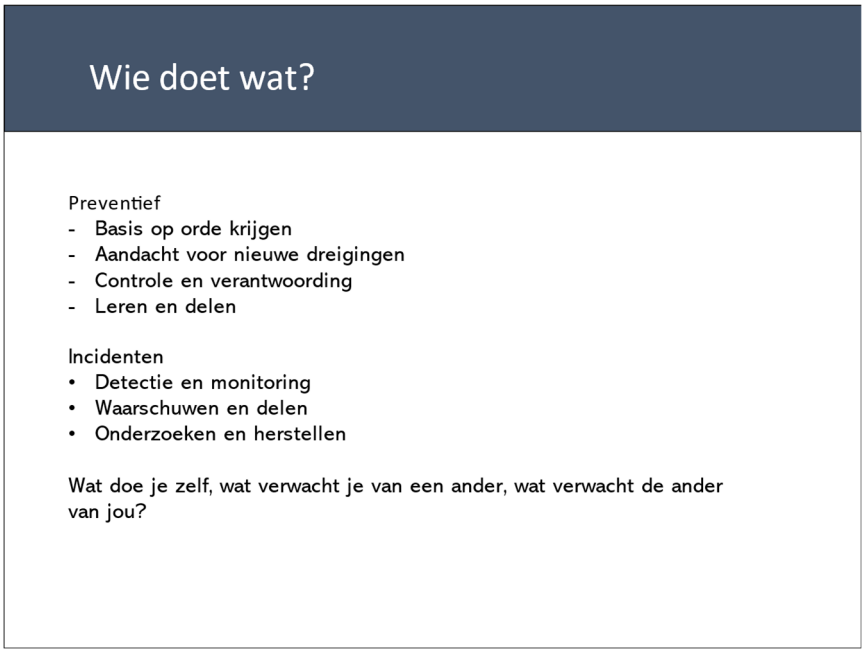
- Basisbekostiging: je moet wel de middelen hebben om een bepaald niveau te kunnen betalen. Het is een afweging die elk schoolbestuur moet maken. Daarbij is het heel belangrijk dat je kan uitleggen waarom het zo is.
- Het is prettig als de overheid wel kaders geeft, de randen van het zwembad aangeeft en zorgt voor voldoende financiering en tijd. Binnen heldere kaders kun je binnen een sector zelf afspreken wat je ambitieniveau is en dat meten. Die afspraken zijn er al, koepels hebben daar een sturende rol in, bijvoorbeeld in het hbo en er is een groeipad tot 2027 geformuleerd voor po/vo.
- Een normenkader kan helpen om veel te standaardiseren. Sommige dingen moeten juist wél op een heel hoog niveau geregeld worden. We moeten vaart zetten, maar je kunt niet iedereen overvragen. Een idee: Zorg voor geoormerkte gelden in het po (mensen, capaciteit, geld). Als ze het geld niet gebruiken moet het terug.
- Sommigen opperen een wet met minimumeisen. Hiermee dwing je alle scholen mee te doen. Een verplichte APK voor de ICT instellen. Anderen zijn juist bang voor te algemene oplossingen: wetgeving maakt het onderwijs niet veiliger. Dit zou het sluitstuk moeten zijn en niet het begin. Wel in de wet vastleggen wie verantwoordelijk is voor welk stuk.

Verantwoording afleggen

- De inspectie wordt gemist op dit dossier. Cyberveiligheid is geen specifiek onderwerp tijdens de onderzoeken. Wel is cyber belangrijk voor de continuïteit van het onderwijs en vanuit die optiek past het ook binnen het gesprek met een school. Maar inspecteurs zijn geen IT-auditors. De inspectie zou ook meer de rol van sparringpartner moeten hebben, vooral ook in crisistijd. De balans tussen wat er nodig is en wat werkbaar is blijkt wel lastig. Hier zou een rol voor de inspectie kunnen liggen.
- Er zou een stelselonderzoek in het po/vo moeten plaatsvinden. Dat zou gebruikt kunnen worden om schoolbesturen te stimuleren hiermee aan de slag te gaan.
- Een bestuurder vertelt dat hij al jaren hierop bevraagd wordt door zijn accountant. Voorstel is om dit onderwerp concreter in het jaarverslag op te laten nemen (verplichten?).
- Oppassen dat we ons niet gaan richten op verantwoording over de normkaders, dat is al snel een papieren werkelijkheid. Ook er op letten dat besturen geen standaard plannen gaan overnemen die in de praktijk niet toegepast worden.

Waarschuwen en delen

- Er is een idee voor een algemene noodknop voor de sector waar iedereen gebruik van kan maken. Hierdoor kun je ook snel informatie met elkaar delen.
- Een dienst inrichten met ondersteuning op praktisch niveau. Dan hoeft niet elke school het wiel opnieuw uit te vinden.
- Waar vind je informatie over bedreigingen en hacks, het kost veel moeite om dat allemaal zelf bij te houden. Bij wie moet ik zijn als bestuurder?



Dia 3 Wie doet wat: verschillende fases en verwachtingen

Sessie 3: Data delen, van wie zijn de gegevens?

Bij dit onderwerp is een inleiding gegeven door een inspecteur systeemtoezicht van de Autoriteit Persoonsgegevens (AP). De handout van de presentatie is opgenomen vanaf pagina 40.

De AP en belangrijke documentatie m.b.t. privacy- en gegevensbescherming

- De AP is de onafhankelijke toezichthouder op het gebied van privacy- en gegevensbeschermingsrecht. De AP houdt toezicht op de naleving van de Algemene Verordening Gegevensbescherming (AVG).
- De AP heeft zowel een stimulerende als een handhavende taak. Het is belangrijk om hierin een balans te vinden. Waar stopt stimulerend toezicht en waar begint handhavend toezicht? Zo heeft de AP advies uitgebracht in het kader van Google Workspace (zie ook slide 5) om de zaken op orde te brengen. Dit beperkt zich niet tot Google. Advies aan de onderwijssector om meer grip op privacy te krijgen, het had net zo goed een andere leverancier kunnen zijn.
- Deelnemers geven aan dat ze behoefte hebben aan een follow-up van meldingen die ze bij de AP doen.
- Belangrijke documentatie op het gebied van privacy- en gegevensbescherming:
    - Verwerkersovereenkomst: de overeenkomst tussen degene die de persoonsgegevens verwerkt en degene die kan worden aangemerkt als de verwerkingsverantwoordelijke. De rolverdeling tussen deze partijen wordt duidelijk in de verwerkersovereenkomst.
    - Data protection impact assessments (DPIAs). Het uitvoeren van een DPIA maakt inzichtelijk welke risico's er verbonden zijn aan o.a. het gebruiken en/of delen van persoonsgegevens. Ook worden maatregelen aangereikt om de risico's te verkleinen.
    - Register van verwerkingen: vaak een verplichting onder de AVG. In dit register wordt informatie opgenomen over welke persoonsgegevens verwerkt worden, de grondslag/het doel van deze verwerking, contactgegevens van de onderwijsinstelling, de bewaartermijn, welke maatregelen genomen zijn t.b.v. beveiliging en met wie de gegevens gedeeld worden (binnen of buiten de EU) etc.

Datadelen – verantwoordelijkheid, bewustzijn en (preventieve) maatregelen

- Twee van de uitgangspunten bij datadelen: risicogebaseerd en eigen verantwoordelijkheid.
    - Risicogebaseerde benadering: hoe hoger de risico's, hoe zwaarder de plichten/hoe beter de maatregelen. In onderwijs bijvoorbeeld: gegevens van kinderen, gevoelige gegevens, vormen indringend beeld van kinderen.
    - Eigen verantwoordelijkheid en accountability: zelf bepalen wat deze risico's zijn. Eigen afweging, open normen. Contextafhankelijk. Plus: aantoonbaar voldoen aan de AVG.
- Het is van belang dat onderwijsinstellingen datastromen in kaart brengen en het overzicht behouden.
- Daarnaast is het belangrijk om *vooraf* te bepalen welke beschermingsmaatregelen je kunt nemen.

- Privacy- en gegevensbescherming is een taak van iedereen binnen een onderwijsinstelling, dus niet alleen van de ICT-afdeling en/of de bestuurder.
- Het is van belang te weten welke systemen en applicaties gedownload/aangekocht zijn en gebruikt worden. Dit is van belang om de risico's te kunnen inventariseren.
- Het zijn veelal de grote besturen die een separate privacy functionaris hebben. Op kleinere scholen wordt het onderwerp privacy veelal opgepakt door één van de docenten of de directeur, aangezien er niet genoeg budget is voor een separate privacy functionaris.
- Op dit moment zijn de bewaartermijnen van documenten met leerlinggegevens en diploma's onbekend. Er is hierover voor het funderend onderwijs nog niets vastgelegd in een selectielijst.[4] De koepel van hogescholen, de Vereniging Hogescholen (VH) heeft daarentegen wel een selectielijst vastgesteld.[5]
- Deelnemers geven aan dat de bewustwording binnen de onderwijssector laag is; aan online e-learning doen percentueel weinig medewerkers mee. Binnen teams op scholen is soms sprake van naïviteit: we doen het al zolang zo, het zal wel goed zijn.
- Momenteel wordt er gewerkt aan een normenkader voor het funderend onderwijs.[6] Dit kader wordt begin 2023 gepubliceerd. Voor de inwerkingtreding zal een implementatietermijn van kracht zijn. Deelnemers geven aan dat dit veel tijd kost. De focus ligt bij verschillende onderwijsinstellingen niet bij het normenkader maar bij onderwijs, tijd ontbreekt. Ga de dialoog met de raden hierover aan.
- Bij wie ligt de verantwoordelijkheid voor veilig digitaal onderwijs? De leverancier? Het bestuur? Bij ketenpartners? Het is een gezamenlijke verantwoordelijkheid!
  Adviezen:
  - Houd structureel (jaarlijks) een grote digitale schoonmaak.
  - Leg de basisaanpak in beleid vast, met daarnaast schoolspecifieke uitwerking + afspraken.
  - Stel beleid op voor gebruik van toegestane ICT-middelen en applicaties/systemen - dit t.b.v. dataveiligheid. Zoek naar spelregels.
  - Houd structureel de integriteitsverklaringen up-to-date. Neem dit mee in de plan-do-check-act (PDCA) cyclus.
  - Stel leveranciers de vraag of zij een DPIA hebben uitgevoerd.
  - Besteed aandacht aan bewustwording binnen de eigen organisatie. *Gratis bestaat niet:* kost een applicatie geen geld, dan betaal je waarschijnlijk met je persoonsgegevens/data.
  - Druk in een aanbesteding de wens uit voor een AVG-certificaat; voor zowel leverancier als afnemer.
  - Zoek een balans tussen de inspanning en de kosten die de inspanning met zich meebrengt. Afstemming is cruciaal.

[4] Zie: https://www.poraad.nl/schoolontwikkeling/digitalisering/ict-organiseren/wettelijke-bewaartermijnen-voor-openbaar
[5] Zie: https://www.verenigninghogescholen.nl/kennisbank/vereniging-hogescholen/artikelen/selectielijst-hogescholen-versie-2022
[6] Zie: https://www.rijksoverheid.nl/documenten/kamerstukken/2022/07/14/verhogen-digitale-veiligheid-onderwijs-en-onderzoek, p. 2

Casus: Digitale leermiddelen

Belangrijk om het volgende in beeld te hebben:

- Welke digitale leermiddelen/applicaties binnen de onderwijsinstelling gedownload zijn en gebruikt worden.
- Welke gegevens van leerlingen/studenten/personeel worden gedeeld met o.a. de leverancier en de bijbehorende privacy risico's.
- De gemaakte afspraken met leveranciers.

- Binnen het onderwijs worden legio verschillende apps en software gebruikt. Dat kan het onderwijs helpen, maar wees je bewust dat bij het gebruik mogelijk persoonsgegevens worden verwerkt. Naast NAW-gegevens o.a. ook: locatie, data over het gebruik. Daarmee is het mogelijk om indringende patronen af te leiden: wat is het niveau van de leerling/student? Wanneer wordt de app gebruikt? Vanaf welk IP-adres en locatie?
- Doel van de AP is niet afschrikken maar bewust maken van deze privacyvraagstukken en de AVG-verplichtingen. Leerlingen, studenten, ouders en personeel mogen er vanuit gaan dat onderwijsinstellingen goed met hun persoonsgegevens omgaan. Met name wanneer een onderwijsinstelling andere partijen inschakelt.
- De ambitie van hogescholen is om schaduwsoftware tegen te gaan. Zou dit ook voor andere instellingen moeten gelden? Hoe gaat u daar mee om?

Sessie 4: Ketensamenwerking

Jasper Nagtegaal, Hoofd Digitale Weerbaarheid bij het Agentschap Telecom[7], gaf een inleiding. De handout van de presentatie is opgenomen vanaf pagina 43.

Ketensamenwerking roept bij de aanwezigen verschillende associaties op. De rode lijn is dat men in het onderwijsveld te maken heeft met erg veel ketenpartners en zich niet altijd bewust is van de mogelijke risico's; men vraagt zich ook af wie er verantwoordelijk is voor veilige data uitwisseling.

Ontwikkelingen en kenmerken

- Er vindt door digitalisering een verschuiving plaats in de keten: van analoog naar digitaal. Digitalisering brengt meer en nieuwe uitdagingen met zich mee. Veelal bestaan er verbindingen in en tussen verschillende digitale ecosystemen zonder dat men zich hiervan bewust is.
- De impact van hacks wordt steeds groter, juist door de verwevenheid van veel partijen. Het is belangrijk om je bewust te zijn van de afhankelijkheden en dreigingen.
- Ketens veranderen. Klassieke vorm, zoals supply chain en outsourcing, bestaan nog steeds. We zien steeds meer combinaties waarin partijen gezamenlijk bijdragen aan een ecosysteem. Elke partij voegt een specialisme toe aan de waardcreatie.
- Een keten is zo sterk als de zwakste schakel. Zie bijvoorbeeld de 'log4j-kwetsbaarheid'[8].
- Soms hebben partijen een unieke positie ook binnen het onderwijs. Zo worden de inschrijvingen en collegegeldbetalingen in het bekostigde hoger onderwijs door Studielink verwerkt.
- Europese wetgeving is in de maak. Onder andere de Cybersecurity Act; introduceert certificeringsschema's voor verschillende producten en diensten, waaronder cloud en de Cyber Resilience Act; introduceert eisen aan digitale producten op het gebied van security en life-cycle management. Op deze manier wordt het voor bedrijven en organisaties eenvoudiger om een geïnformeerde keuze te maken over een dienst of product.
- Wie heeft de regie op alle gegevens? Waar leg je de verantwoordelijkheid neer? Bij de overheid?

Afhankelijkheid leveranciers, rol onderwijsinstelling

- Supply chain --> wie levert wat? Steeds meer onderlinge afhankelijkheid --> dit leidt tot complexiteit en kwetsbaarheid. Leveranciers weten soms zelf niet wat er achter hun product zit. Het vraagt daarom veel vertrouwen in alle partijen.

[7] Vanaf 1 januari heet het Agentschap Telecom de Rijksinspectie Digitale Infrastructuur.
[8] Uit factsheet IvhO: In december 2021 deed zich een groot probleem met Log4J voor. Dit was een kwetsbaarheid in veel verschillende softwareprogramma's waar toen nog geen oplossing voor was. Eerst was onbekend in welke programma's het was toegepast. Om het onderwijs te helpen heeft Kennisnet alle in het primair en voortgezet onderwijs gangbare digitale onderwijsproducten geanalyseerd en een openbare lijst gemaakt van softwareprogramma's die kwetsbaar waren voor Log4J. Ook als de leverancier hiervoor een oplossing had stond dit erbij. Het was mooi om te zien dat er geen lidmaatschap van Kennisnet nodig was om deze informatie te kunnen zien; die was voor iedereen toegankelijk. Kennisnet volgde hiermee de werkwijze van de Nationaal Coördinator Terrorismebestrijding en Veiligheid. SURF heeft vervolgens een vergelijkbare lijst voor het middelbaar beroepsonderwijs en hoger onderwijs gemaakt.

- Wat zijn de ketens en wat zijn de afhankelijkheden binnen deze ketens? Afnemers vertrouwen leveranciers met hun data. Bewustzijn van deze complexiteit is belangrijk!
- Er is geen sprake meer van één leverancier, maar meerdere (toe)leveranciers in één keten. Ecosystemen zijn de norm nu.
- Leveranciers worden steeds groter en sterker en daardoor wellicht minder transparant? Sommige diensten worden enkel aangeboden door techreuzen o.a. Microsoft en Google. Zoek de samenwerking op en stel kritische vragen en maak je zorgen duidelijk! Houd de betrouwbaarheid in het oog en blijf vragen om transparantie. De dialoog is belangrijk.
- Deelnemers vragen zich af of het voeren van de dialoog niet onmogelijk is voor scholen zelf. Wordt een school wel als gesprekspartner geaccepteerd bij grote leveranciers? Dan ben je toch afhankelijk van koepels (bijv. UNL, MBO-Digitaal en de VO-raad) die gezamenlijkheid kan organiseren. Bepaalde certificeringen zouden kunnen helpen. Zo wordt in Europees verband voor het onderwijs gesproken over EDU-V.
- Certificering of standaarden helpen de keten voldoende kwaliteit te leveren. Uniformeren in IT kan hier bij helpen, ook op instellings- of schoolniveau kunnen eisen gesteld worden aan de voorkant, bijvoorbeeld bij de keuze van systemen. Dan moet je er wel op kunnen vertrouwen dat het systeem achter die certificering ook werkt, toezichthouden daarop is noodzakelijk.
- Dit vraagt ook om gesprek binnen onderwijsinstellingen. Een meer uniforme aanpak kan door docenten worden gepercipieerd als inperken van autonomie.
- Risico's in ketens, waaronder gegevensuitwisseling, is niet uniek voor het onderwijs. Bespreek ook buiten de bubbel van het onderwijs hoe anderen organisaties hier tot een aanpak komen.
- Ga op zoek naar maatwerkdienstverleners.

Binnen de eigen organisatie

- Hoe zorg je dat je 'in control' bent en blijft als bestuurder? Ben je je bewust welke apps door welke afdelingen gebruikt worden? Hoe zorg je ervoor dat er geen vergeten systemen zijn? Zijn de risico's in kaart gebracht? Welke risico's accepteer je en welke niet?
- Bewustwording is heel belangrijk. Ben je in staat om de risico's te inventariseren? Welke afhankelijkheden en dreigingen zijn er in ketens waar de organisatie deel van uitmaakt? Neem medewerkers mee. Leg bijvoorbeeld uit wat de cloud is en hoe het werkt. Alle lagen van de organisatie moeten meegenomen worden, ook bijvoorbeeld inkoop en de mensen die ergens mee moeten werken. En: kwaliteit IT meenemen in de jaarlijkse PDCA-cyclus.
- Maak back-ups!
- Vraag je af wat de behoefte is in de organisatie en wees bewust wat de functionaliteit is van de (huidige) systemen. Data uitwisselen via ketens is nodig, maar de wetgeving is vaak zó strikt of zó ingewikkeld, dus onwerkbaar. Daardoor zoekt men buiten de systemen om en dit werkt risico's in de hand. Zijn de kaders te complex? Dit kan leiden tot weerstand, wat het downloaden/gebruiken van eigen systemen in de hand kan werken. Zorg voor goede afwegingen zodat maatregelen proportioneel zijn en ook zo worden ervaren. Leg tevens het belang van gemaakte afspraken uit.
- In het onderwijs, zeker in het speciaal onderwijs, wordt gebruikt gemaakt van verschillende (oudere) IT-systemen of applicaties die niet voldoen aan de huidige beveiligingsnormen. Deze systemen of applicaties zijn nodig om leerlingen met

specifieke behoeften te kunnen ondersteunen. Het gaat om aanpak in een niche voor 1 of 2 leerlingen. Het is zoeken naar oplossingen (bijvoorbeeld standalone computer) om dit aan leerlingen aan te bieden.

- Advies: houd ieder jaar een grote digitale schoonmaak. Dit gaat niet alleen om assetmanagement: hoe ziet het IT-landschap eruit, welke toepassingen worden allemaal gebruikt, maar denk ook aan speciale toepassingen voor een beperkte groep leerlingen of studenten met extra ondersteuningsbehoeften. Check op gebruikersrechten; zijn er autorisaties die ingetrokken hadden moeten worden?
- Hoe houd je zicht op waar medewerkers allemaal mee werken? Een deelnemer geeft als tip elk half jaar te inventariseren wat er is ingekocht zonder vooraf overleg met inkoop/IT. Nu dit bij de onderwijsinstelling langer wordt gedaan weten medewerkers elkaar te vinden en wordt inkoop/IT vaker betrokken bij de aankoop.
- Advies: zoek hulp, zoek de verbinding op. Organiseer het in beleid.

Conclusie: Wees je bewust van de vele schakels in de keten (ecosystemen) en dat dit zorgt voor complexiteit, kwetsbaarheid en afhankelijkheid. Zorg dat je zicht hebt en houdt op alle systemen die gebruikt worden, voer jaarlijks een grote digitale schoonmaak uit en zoek samenwerking op. Stel vragen, blijf kritisch op de risico's en stap uit je eigen bubbel.

De Nederlandse Cybersecuritystrategie 2022-2028 is hier te downloaden.
tekst

Sessie 5: Help ik ben gehackt!

Voor dit onderwerp gaven (voormalige) bestuurders van de Universiteit Maastricht, het Openbaar Onderwijs Groningen en het Staring College een inleiding over een hack die hun onderwijsorganisatie is overkomen in respectievelijk december 2019, maart 2020 en februari 2021. In aanvulling op de plenaire presentatie door Mark Koek gingen ze in een openhartig gesprek in op wat zo'n gebeurtenis voor impact had en nog heeft op de organisatie en voor welke keuzes je als bestuur komt te staan.

Crisisafhandeling

Onderwijsinstellingen die getroffen zijn door een hack komen in de crisisafhandeling voor keuzes te staan die afwegingen vergen tussen opsporingsonderzoek (wat is er gebeurd), (spoedig) herstellen van de IT, mogelijkheden om de reguliere processen waaronder het onderwijs door te laten gaan.

Opsporingsonderzoek (forensisch onderzoek)

- Je kunt dit niet zelf oplossen: zoek externe hulp van (forensisch) specialisten.
- Ga niet uren, dagen, weken lopen zoeken naar of er een fout is gemaakt; handel bij vermoeden van een hack direct en schakel professionals in.
- Zodra duidelijk is dat er een hack is geweest niet meer proberen het zelf op te lossen, dit kan later het onderzoek namelijk bemoeilijken.
- Zorg dat je als bestuurder op de hoogte bent van de situatie zonder professionals in de weg te lopen.
- Deel informatie over de aanval (IoC's = Indicators of Compromise) uit het onderzoek met andere (onderwijs)partijen zodat ze gericht kunnen zoeken of er voorbereidingen voor een aanval plaatsvinden.

Crisisorganisatie

- Richt als eerste een crisis (management) team in.
- Zorg voor een actueel calamiteitenplan. Het crisisteam moet vooraf bepaald zijn. Zorg ook voor een organisatieprotocol.
- Weet wie je moet waarschuwen van je externe contacten (Politie, Autoriteit Persoonsgegevens, Ministerie, regionale partijen zoals gemeente, Inspectie van het Onderwijs, NCSC, etc).
- Zorg voor een veilige communicatiemogelijkheid voor het calamiteitenteam en naar anderen in de organisatie die vragen hebben. Dit kan bijvoorbeeld een whatsapp groep zijn, heb die al gereed. De mogelijkheden om medewerkers, leerlingen en studenten te bereiken hangt af van wat er is geraakt bij een hack. Bij één hack bleek de website nog toegankelijk en kon als middel dienen.
- Bij grote hack: bereid je voor op de pers, hierbij is externe hulp nodig.
- Wees zo open en transparant mogelijk over wat er speelt, voorkom grote paniek, daar valt niet op te sturen.
- Er is gekozen om alles open te communiceren, dit heeft veel goeds opgeleverd. Ook heeft de Universiteit Maastricht daarna erg veel werk gemaakt van het bewust maken van andere instellingen door voorlichting aan te bieden en te komen vertellen hoe groot de impact is geweest op alle betrokkenen.

- Bescherm je IT-afdeling, laat ze hun werk doen en ga niet in de weg lopen.

Crisisbesluitvorming
- Bestuurlijke keuze: focus op opsporing of herstel. Het laatste wist mogelijke sporen.
- Duivels dilemma: kosten en gevolgen afwegen van betalen of zelf oplossen door opnieuw op te bouwen, waardoor onderwijs en andere reguliere processen enorme vertragingen oplopen of zelfs opnieuw gedaan moeten worden.
- De keuze om wel of niet te betalen is een onmogelijke keuze, maak een afweging op basis van een risicoanalyse. Het blijft een duivels dilemma, maar wees transparant over de motivatie om het wel of niet te doen.
- Er werd ontraden te betalen maar hier is toch toe besloten. Door te betalen steun je echter de hackers, maar zelfs met de sleutels duurde het nog 7 tot 8 dagen voor de belangrijkste systemen weer op orde waren, totale herstel duurde nog veel langer.
- Niet alle drie de instellingen hebben de losgeldeis betaald. Een van de keerzijden bij het niet betalen is het verlies van materiaal. Binnen een onderwijsinstelling was de hack beperkt tot een cluster van enkele scholen. Bij deze scholen is sprake van verlies van onderwijsmateriaal inclusief backups. Dit heeft het voor de betreffende onderwijsteams die materiaal kwijt zijn grote impact gehad.

Herstelfase

Na de initiële fase waarin vanuit de crisisorganisatie wordt gewerkt is afgerond, gaat het werk weer over in de reguliere processen. Wel is er nog een fase van herstel waarin in het bijzonder de IT-afdeling nog aan de slag is met controle, herstel of herbouw. Voor hen gebeurt dit naast de reguliere werkzaamheden. De overige (primaire)processen hebben weer doorgang en merken hier minder van.

Impact op de organisatie
- Herstel kost heel veel tijd en geld, zelfs als je losgeld betaalt.
- Onderschat, naast de kosten, de impact niet op mensen. Mensen worden echt geraakt, voelen zich zelfs verantwoordelijk. De impact is echt gigantisch. In het bijzonder: de impact op de eigen IT'ers is groot, die voelen zich in hun eer geraakt, onderschat dit niet.
- Werkelijke kosten is niet het losgeld maar de aanpak tijdens de hack en herstelkosten daarna, die zijn factoren hoger dan het losgeld. Alle teruggezette gegevens dienen bijvoorbeeld te worden gecontroleerd voordat ze weer vrij worden gegeven (wasstraat).
- Gedurende lange tijd (>1 jaar) is monitoring ingekocht via de externe partij die betrokken was bij het forensisch onderzoek gedurende de crisisafhandeling en soms ook nu nog gecontinueerd. Universiteiten en hogescholen werken aan een gezamenlijke monitoring.

Bewustzijn in de hele organisatie
- Een crisis doet iets, maar het effect ebt ook weer weg. Zo neemt de bewustwording kort na een hack enorm toe, maar zwakt later ook weer af.
- Wijs iedereen op de eigen verantwoordelijk en (digitaal) gedrag. Dit is niet iets eenmaligs, maar moet doorlopend plaatsvinden.

- Zorg dat je als bestuurder op de hoogte bent van de situatie in je onderwijsinstelling, liefst op basis van een quick scan; er is op dit moment weinig instrumentarium beschikbaar.
- Multi Factor Athenticatie (MFA) werkt echt! Na een grote hack is dit beter aan de gebruikers te verkopen. Invoering stuit vaak op verzet: men vindt het gedoe.
- Realiseer je dat cybersecurity en privacy in elkaars verlengde liggen.

Lessen

Beleid(safweging)

- Wees je bewust van het feit dat je nooit 100% veilig kunt zijn, het is vaak ook een kostenafweging, maak hierin transparante keuzes.
- Iedereen kan worden gehackt, groot of klein en de kosten om de risico's te beperken zijn fors. Zo zijn kosten van bijvoorbeeld monitoring hoog maar dat geldt ook voor de kosten om te herstellen na een hack.
- Gehackt worden in de praktijk: de dag voor Kerst of een vakantieperiode lopen we het meeste risico. Wees je bewust dat er dan minder mensen zijn om op signalen te reageren.
- Voorkomen is beter dan genezen: zorg voor voldoende middelen en haalbare ambities. Soms gaan technische keuzes voor (om achterstanden te voorkomen) en moeten de 'leuke' dingen even wachten.
- Het uitspreken van een gezamenlijk ambitieniveau op het normenkader zorgt voor focus. Dit is gericht op verbeteren en verhogen van de weerbaarheid. Realiseer je dat de score van bijvoorbeeld niveau 3 nu over enkele jaren 2 zal zijn. Blijf aandacht houden, investeren en innoveren.

Informatiebeveiliging en privacy

- Regel je monitoring in, kost geld, maar zo kan er in een vroeg stadium verdachte activiteit worden ontdekt.
- Laat regelmatig een technische toets uitvoeren door een externe partij (gericht op hardware).
- Realiseer je dat het applicatielandschap kwetsbaar blijft.
- Oude niet meer gebruikte accounts vormen een risico, zorg dat je regelmatig schoont. Dergelijke accounts (zeker met beheerrechten) zijn een geliefde buit voor hackers.
- Met name voor kleinere besturen is er hulp (het liefst vanuit de sector) noodzakelijk om dit goed te kunnen implementeren. Er is behoefte om te weten wat ze (nog) meer moeten doen dan er nu wordt gedaan. Doet iedere (kleine) instelling een cyber security screening en hoe weet ik of dit voldoende is?
- Een voorbeeld van een aanwezige onderwijsinstelling is de inrichting van gezamenlijke monitoring en kennisuitwisseling van met enkele (regionale) onderwijsinstellingen.

Cyberaanvallen en incidenten

Bij sommige deelnemers leeft de vraag: door hoeveel cyberaanvallen wordt het onderwijs getroffen? En mogelijk de vervolgvraag: is het onderwijs kwetsbaar(der) dan andere sectoren in Nederland? Hierover zijn geen betrouwbare cijfers bekend. Uit verschillende rapportages zoals het Cybersecuritybeeld Nederland, het Cyberdreigingsbeeld Onderwijs en

Onderzoek en Datalekrapportage van de Autoriteit Persoonsgegevens blijkt dat het aantal jaarlijks bekende incidenten toeneemt. Gedurende de rondetafelbijeenkomsten zijn verschillende incidenten genoemd bij andere instellingen. Ook tijdens de sessie Help ik ben gehackt.

- Al enige jaren geleden vond een hackaanval plaats via DDOS waardoor systemen 2 dagen onbruikbaar waren. Het bleek door een leerling ingekocht te zijn voor €25! Afgetrapt via de telefoon van een andere leerling die door de aanvaller was gehackt.
- Een aanval via het kassasysteem van de cateraar. Bij de eigen onderwijsinstelling was dit op tijd ontdekt, maar had bij andere instellingen wel schade veroorzaakt: het kan dus ook via externe partners komen.
- Zoals uitgelegd gedurende de plenaire start vindt een aanval in stappen plaats. Zo bleek uit het forensisch onderzoek dat de hackers bij de aanval op de Universiteit Maastricht al enige maanden eerder ingebroken hadden. Daarna zijn voorbereidende handelingen getroffen voordat (aan begin van de vakantieperiode) de ransomware aanval werd uitgevoerd.

Conclusie

Tijdens alle vier gesprekken zijn veel verschillende vragen gesteld. De ervaringen die gedeeld zijn door de bestuurders die een hack meemaakten heeft veel indruk gemaakt. Er werd heel open en eerlijk gesproken over keuzes waar je als bestuurder voor komt te staan. Die vallen niet altijd mee en doen iets met verschillende mensen in de organisatie. Er is geen juiste keuze. Van belang: wees open en transparant, neem alle zorgen serieus. Houd regie op het proces van de crisisafhandeling en heb ook oog voor de impact later tijdens de herstelfase.

Panelgesprek / terugkoppeling

De bijeenkomsten zijn afgesloten in de vorm van een korte terugkoppeling per sessie in Zwolle en een panelgesprek in Den Bosch.

Sessie 1 Hoe cyberweerbaar is mijn onderwijsinstelling?
Stelling: Het is voor onderwijsinstellingen duidelijk welke maatregelen ze moeten doorvoeren om hun cyberweerbaarheid te vergroten

- Dit is nu voor onderwijsinstellingen nog niet het geval, blijkt uit de discussie in de sessie.
- Een vraag die speelt is: wie bepaalt de norm? Kennisnet is in samenwerking met andere partijen bezig met het opstellen van definities en een minimumset van maatregelen en procedures. In samenspraak zal moeten worden afgesproken wat 'veilig' is: waar moet een onderwijsinstelling aan voldoen?
- Als het normenkader er is, kost het nog een behoorlijke tijd om de implementatie bij scholen op orde te krijgen. Een afgesproken minimumset kan niet direct van kracht zijn.
- Er is veel bereidheid om werk te maken van cyberveiligheid. Deelnemers aan deze bijeenkomsten zijn zich bewust van het belang. Wel is het belangrijk om aandacht te besteden aan het creëren van meer bewustwording binnen de gehele onderwijssector, bij alle scholen, ongeacht sector en schaalgrootte.
- Het werk van bestuurders is complexer geworden. Bestuurders zijn verantwoordelijk, maar hebben bepaalde inhoudelijke kennis niet.

Sessie 2 Wie is verantwoordelijk voor veilig digitaal onderwijs?
Stelling: Er dient een bij wet verplicht normenkader te komen voor de gehele onderwijssector

- Onderwijsinstellingen zijn al verantwoordelijk, immers er is wettelijk geregeld dat het bestuur de continuïteit van het onderwijs moet waarborgen.
- Er is wel behoefte aan meer duidelijkheid over wat er door wie moet worden gedaan, hoe dit dient te gebeuren en wanneer. Hierbij zou een wettelijke basis uitkomst kunnen bieden.
- Er is veel diversiteit tussen verschillende organisaties. Ondersteuning van het Ministerie van Onderwijs, Cultuur en Wetenschap (OCW) is gewenst en nodig.
- Gezien de verwevenheid in het onderwijs, ook tussen onderwijssectoren, kan het opstellen en verplichten van een normenkader helpen. Wenselijk is dat hetzelfde uitgangspunt voor alle onderwijsinstellingen ongeacht sector en schaalgrootte geldt.
- Er zijn mooie voorbeelden gedeeld door onderwijsorganisaties die het onderwerp cyberveiligheid op de agenda hebben staan. Belangrijk is dat we van elkaar (blijven) leren.

Sessie 3: Data delen, van wie zijn de gegevens?
Stelling: Het goed inregelen van IB&P (Informatiebeveiliging & privacy) is de verantwoordelijkheid van mijn softwareleverancier.

- De AVG is er duidelijk over: de afnemer is verantwoordelijk.
- Hoe moeten we hiermee aan de slag? Gezamenlijkheid kan helpen. Partijen als SURF en SIVON kunnen behoeften van het onderwijsveld in kaart brengen en samen met het onderwijs voorwaarden stellen aan leveranciers.

- Gezamenlijk optrekken helpt ook om te voorkomen dat iedereen zelf opnieuw het wiel probeert uit te vinden.
- Binnen onderwijsinstellingen is het van belang om (periodiek) te inventariseren welke systemen aangeschaft zijn en welke daadwerkelijk gebruikt worden. Docenten zien handige tools die ze willen gebruiken, maar zijn die wel veilig? Dit raakt aan de discussie over de sturingsvraag en de autonomie van docenten.
- Als instelling wil je open zijn en met elkaar en de buitenwereld communiceren. Dat levert spanning op tussen de primaire doelstelling (onderwijs verzorgen) en het waarborgen van een veilige online omgeving (cyberveiligheid). Er moet gezamenlijk met medewerkers een balans gevonden worden. Bewustwording vergroten – bijvoorbeeld door te illustreren wat de gevolgen van een grootschalig incident voor het onderwijsproces kunnen zijn. Dit is een continue discussie.
- Het gedrag van (bijvoorbeeld) docenten is niet uniek, alle sectoren hebben hiermee te maken. Je werk als bestuurder wordt complexer en vraagt om afwegingen: draagt dit echt bij aan onderwijskwaliteit en wat zijn de risico's op een cyberincident zoals een hack?

Sessie 5 Help ik ben gehackt!
Stelling: Het Nederlandse onderwijs is goed voorbereid op een mogelijke hack.
- Onderwijsinstellingen die met een hack geconfronteerd zijn geweest hebben noodgedwongen goed rondgekeken hoe zij hun cyberweerbaarheid kunnen verhogen. Voor hen is een hack aanleiding geweest om hun cyberveiligheid op peil te brengen.
- Het woord "goed" past hier niet. De gehackte instellingen waren niet voorbereid, dat is nu verbeterd. Maar let op: het is een permanente ontwikkeling om de digitale veiligheid op niveau te krijgen en te houden voor elke onderwijsinstelling.
- Bestuurders zijn ook door anderen benaderd. De ervaring is dat grote bedrijven verbergen dat er een hack heeft plaatsgevonden. Cyberincidenten komen bij instellingen in alle sectoren voor ongeacht de schaalgrootte van de instelling.
- Welke afwegingen je als bestuur maakt kan per geval verschillen. Het is raadzaam om protocollen op te stellen waar je op terug kunt vallen in geval van een hack. Denk hierbij aan het inrichten van crisisteams.
- In het hoger onderwijs zijn maatregelen doorgevoerd aan de voorkant. Een ketenbenadering waarin samen wordt opgetrokken is essentieel; anders is het voor onderwijsinstellingen zelf niet te betalen.
- Problemen die ontstaan door een hack kunnen wel tot twee jaar voortduren voordat zij zijn opgelost. Dat vraagt veel van mensen in een onderwijsorganisatie.
- Betere monitoring in alle onderwijssectoren is noodzakelijk. Dit om vroegtijdig afwijkende zaken te kunnen opsporen en hierop te kunnen reageren. Continue alertheid, 24/7 monitoren, is kostbaar.

Sessie 4 Ketensamenwerking
Stelling: Onderwijsinstellingen zijn zich bewust van cyberrisico's die het werken in ketens met zich mee brengt
- Nee op dit moment niet. Maar dat is niet direct zorgelijk. Dit geldt namelijk niet alleen voor het onderwijs maar voor heel veel sectoren. Belangrijk is dat ketensamenwerking onder de aandacht is. Ook onderwijsinstellingen moeten hier aandacht aan schenken.

- Er ligt een systeemvraag voor het onderwijs: waarin kun je harmoniseren en welke hulp heeft het onderwijs daarbij nodig?
- Er is behoefte aan meer samenwerking met en ondersteuning door onafhankelijke partijen, juist ook om tot goede samenwerking met de grote ICT-partijen te kunnen komen.
- Start met het creëren van bewustzijn, o.a. door het voeren van gesprekken. Ketens worden steeds complexer, waarbij je steeds afhankelijker wordt van andere systemen. Door in gesprek te gaan komen er koppelingen (afhankelijkheden) boven tafel.
- Ga in gesprek over hoe data wordt gedeeld en welke tools worden gebruikt. Regels werken ook om beter geïnformeerd te zijn en zo betere keuzes te kunnen maken.
- Laat horen waar behoefte aan is. Benut de koepels en netwerkpartijen om dit (gezamenlijk) tot uiting te brengen. In alle sectoren ook in het onderwijs moeten voorwaarden gesteld worden aan de ketenpartners. Er is al verbetering zichtbaar, doordat ook vanuit het onderwijs vragen worden gesteld. Maar er is ruimte voor verdere verbetering.

Datum
12 januari 2023

Onze referentie
35528954

Handout Plenaire start

HackDefense

Hoe werken hackers

Over phishing, wachtwoorden en de uitdagingen voor IT en bestuurders

Mark Koek 10-11-2022 m.koek@hackdefense.nl

Wie ben ik

- Oud-leerling van basis- en middelbare school in West-Brabant
- Informatica, Universiteit Leiden
- Oud-NCSC, -Deloitte, -Fox IT
- Oprichter & directeur, HackDefense
  - o.a. actief voor scholengroepen, hogescholen, universiteiten
- Twee kinderen in het middelbaar onderwijs

Wat doet HackDefense

- Ransomware-kwetsbaarheidsanalyses (RKA)
- Applicatie-veiligheidstests (mobiel of web)
- Beveiligingstests van netwerken (Wi-Fi of vast)
- Phishing-simulaties en gebruikerstraining
- Periodiek extern en intern scannen op kwetsbaarheden
- **De IT security partner voor professionele diensten en advies**

CCV CYBER PENTEST

Hackers zijn geen tovenaars

100% preventie is niet mogelijk

Maar het is een hanteerbaar probleem

Remco Pijpers
1d · Edited

En toen hing Malmberg aan de lijn. Klopte het, dat de school via de webshop licenties had besteld ter waarde van een half miljoen Euro?

Oeps.

Met wat rondklikken tijdens de rekenles had een leerling ontdekt hoe je vrij simpel een account kon creëren. Vervolgens was de aankoop snel gedaan. Tienduizend licenties.

De uitdaging

- Net als alle organisaties gebruikt het onderwijs veel IT
- Deze IT is verbonden met het internet
- Boeven buiten, leerlingen/studenten binnen
- De risico's: datadiefstal, onbeschikbaarheid, afpersing, data-integriteit
- De praktijk anno 2022: **ransomware**

Hoe werkt ransomware (1)

Eerste inbraak

Via phishing of via de thuiswerkvoorzieningen

Escalatie

Vanuit het account van een gewone gebruiker een netwerkbeheerder aanvallen

Exfiltratie

Alle data downloaden die je kunt vinden

Hoe werkt ransomware (2)

Backups vernielen

Backupsystemen zoeken en alles wissen

Encryptie

Alle systemen in het netwerk onbruikbaar maken

Afpersing

Losgeld eisen, herstel-sleutel beloven en dreigen met openbaarmaking vertrouwelijke data

Maar wat doe je hier dan tegen?

Concrete technische maatregelen tegen ransomware

- Initiële inbraak: vertrouw niet op wachtwoorden, train medewerkers op phishingmails, update de servers die met het internet verbonden zijn minimaal wekelijks
- Escalatie van inbraak: voorzichtig met Windows Domains (zeer technisch, toch belangrijk), houd het overzichtelijk, houd gebruikersgroepen gescheiden, update alle systemen minimaal maandelijks
- Backups: minimaal wekelijks en bewaar los van het netwerk

Maar wat doe je hier dan tegen?

Bestuurlijke maatregelen voor IT-veiligheid

Bestuur

- Security Officer en Functionaris Gegevensbescherming met voldoende mandaat
  - Hoeft niet full-time, kan gedeeld
- IT-beveiligingsbeleid niet aan IT laten
- Genoeg budget voor IT

IT

- Het moeilijkst te hacken is:
  - Een IT-organisatie die goed weet **wat er draait** en **hoe het werkt**
  - Een IT-organisatie die genoeg tijd heeft voor **basishygiëne**
- Maar laat IT-beleid niet aan de IT-afdeling

Wat niet werkt

- Wachtwoorden (!)
- Alles uitbesteden
- Op papier aan de AVG voldoen zonder praktijktests
- Product kopen (“met deze software bent u 100% veilig!!!”)
- Alleen beleid maken
- Alleen aan de IT’ers overlaten

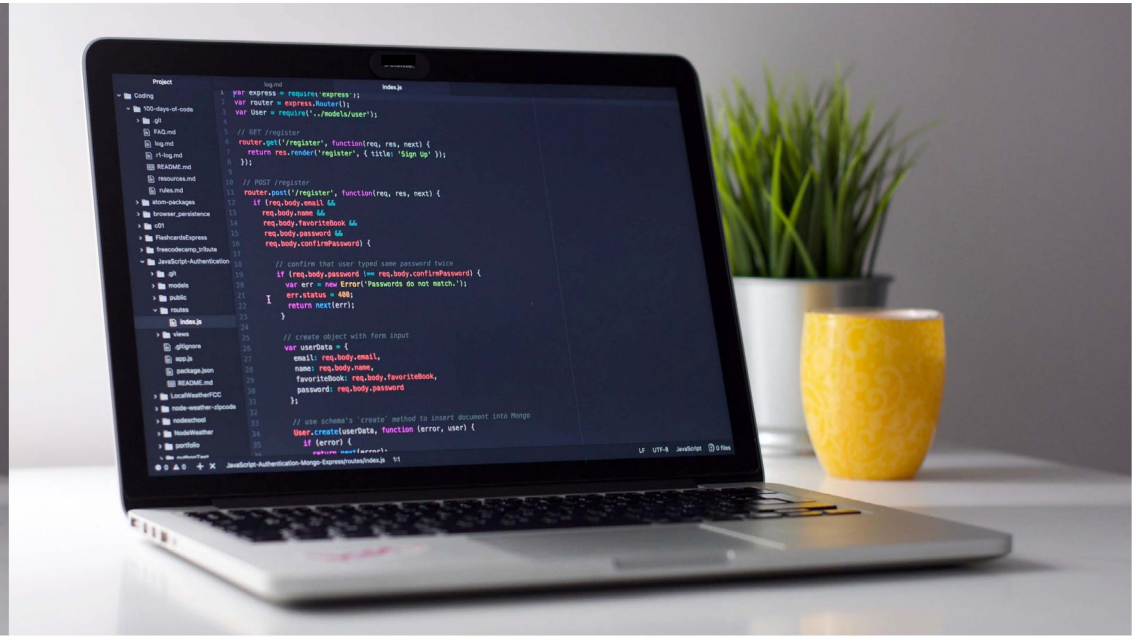
Wat wel werkt

- Multi-factor authenticatie
- Verantwoordelijkheid nemen
- Periodiek onderhoud, testen en: grote schoonmaak
- Beveiliging als bedrijfsproces: voorbereid zijn
- Een helder beleid dat aansluit op de praktijk
- Blije, deskundige IT’ers

Samengevat

Wat kan een onderwijsbestuurder concreet doen om hacking te voorkomen

- Zorg voor voldoende professionele IT-deskundigheid
- Vertrouw op de IT’ers, maar stel randvoorwaarden voor veiligheid
- Beleg verantwoordelijkheden en bevoegdheden in de organisatie
- Jaarlijkse grote schoonmaak
- Let op die wachtwoorden
- Inventaris



HackDefense

IT security, maar dan begrijpelijk

Datum
12 januari 2023

Onze referentie
35528954

Handout Sessie 1

Kennisnet

Hoe cyberweerbaar is mijn onderwijsinstelling?

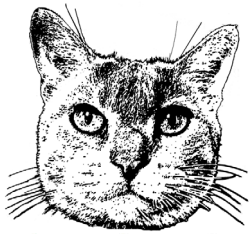
11 oktober 2022

Brenno de Winter & Keiko
Larissa Zegveld & Chris Zintel

Laat ict werken **voor het onderwijs**

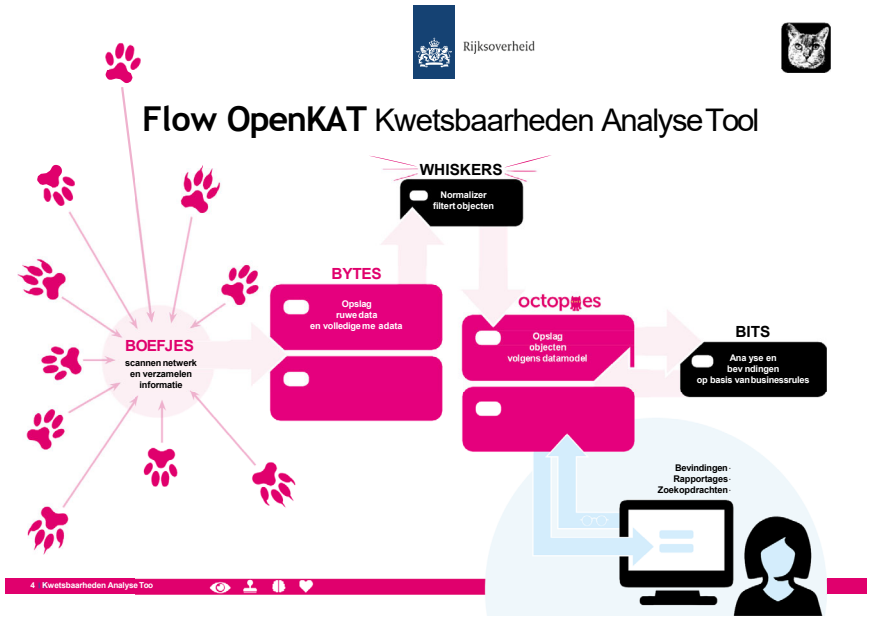
Cyberweerbaar is een keuze en we helpen!

Een bijdrage: Kattenliefde!



- De Kwetsbaarheden Analyse Tool
  - Een tool gemaakt in tijden van Corona-crisis
  - Levert inzicht in die zaken die kwetsbaar maken:
- Technische problemen
- Niet voldoen aan standaarden
- Onveilige praktijken
- Veranderingen in omgevingen

Spelden bij spelden, hooi bij hooi



Findings

11 Findings on example.org

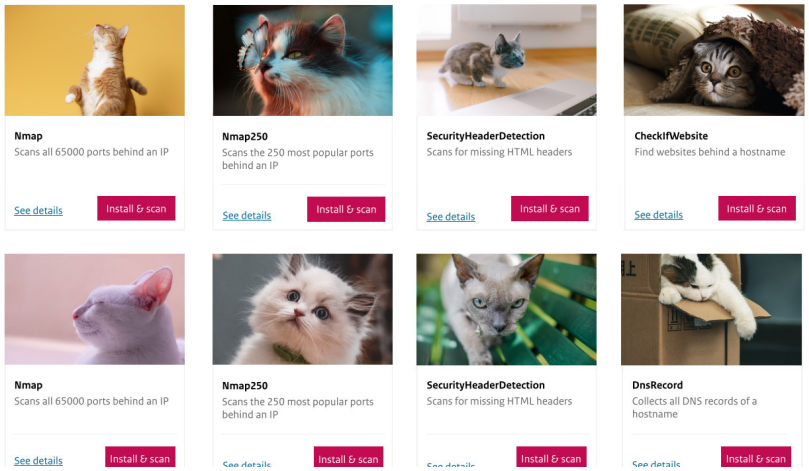
Show filter options

Findings for website https://example-com on 4th of March 2021:

Risk level	Finding type	Occurrences	First known occurence	Status	Details
Critical	Cat has access to passwords	1	March. 4, 2021 5:30pm	New	
Critical	Cat tweeted the passwords	9001	March. 4, 2021 5:30pm	New	
High	Kittens inside the database	12	March. 4, 2021 5:30pm	New	
High	Outdated third party software used	2	March. 4, 2021 5:30pm	New	
High	Inline javascript	15	March. 4, 2021 5:30pm	New	
Medium	Session cookie is valid for too long	1	March. 4, 2021 5:30pm	New	
Medium	Initial administrator password decryptable available in the database	1	Feb. 15, 2021 2:45pm	Known	
Medium	Missing anti-hijacking security measures	1	Feb. 15, 2021 2:45pm	Known	
Low	Incomplete auditlog	1	March. 4, 2021 5:30pm	New	
Low	No automatic referral to https	1	March. 4, 2021 5:30pm	New	
Informational	2-factor authentication currently not required	1	March. 4, 2021 5:30pm	New	

10 Boefjes available

Show filter options



Findings over time

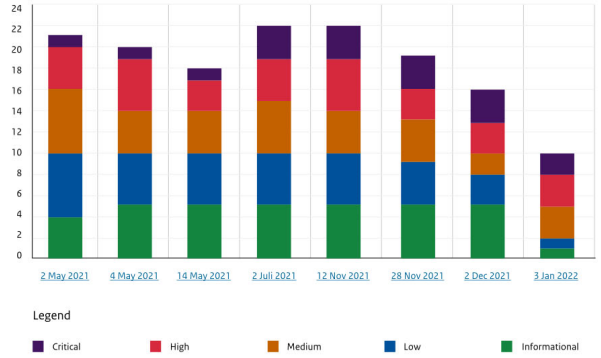
Comparing the current report to previous reports.

Over time issues can arrise or be solved. This graph gives a high overview of the current status compared to previous report(s). Giving insight into the number and type of issues.

Select one or mulitple reports to create a full and indepth comparison report.

Compare reports

Current report compared to previous reports.



Findings

Number of findings compared between:

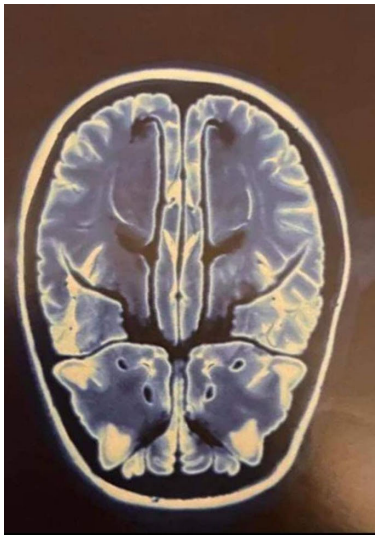
A: Pen Test Report example.org - Mrt. 4 2021 5:30pm - **B:** Pen Test Report example.org - Feb. 15 2021 4:31pm

Severity	Unique findings			Total occurrences		
	Most recent (A)	Previous (B)	Difference	Most recent (A)	Previous (B)	Difference
Critical	2	2	-1	20	25	-8
			+1			+3
			0			**-5**
High	3	3	- 0	12	16	-5
			+ 0			+1
			0			**-4**
Medium	2	3	-2	20	25	-8
			+1			+3
			-1			**-5**
Low	3	6	-3	12	16	-5
			+ 0			+1
			-3			**-4**
Informational	2	1	-1	20	25	-8
			+2			+3
			+1			**-5**

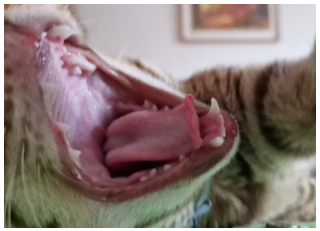
Keiko

- Rapportages
- Gebaseerd op standaarden
- Met verklarende woordenlijsten (als je wilt)
- Bundelt meerdere queries effectief
- Levert door forensische signing onafhankelijke, onweerlegbare rapportages

Een KAT-SCAN



Vragen? Bijvoorbeeld:



- Werkt het KAT-team samen met Kennisnet?
- Wat heeft mijn organisatie eraan?
- Welke van jouw katten zitten in OpenKAT?
- We zien steeds meer regels op ons afkomen, die best ingewikkeld zijn. Hoe helpt OpenKAT?
- Wat is Calvin?

Het funderend onderwijs is onvoldoende veilig

Hoe zadelen we scholen niet alleen op met nóg een probleem, maar zorgen we ook voor een oplossing?

Gecoördineerde aanpak nodig

- **Autoriteit Persoonsgegevens**
  "De AP wil u als stelselvertegenwoordiger van het primair- en voortgezet onderwijs met klem adviseren een pakket aan maatregelen te nemen waarmee wordt bewerkstelligd dat onderwijsinstellingen ook in de praktijk zorgdragen voor veilig onderwijs bij de inzet van digitale middelen."
- **Inspectie van het Onderwijs**
  "Digitale veiligheid kan ook niet worden overgelaten aan de individuele instellingen. Daarom moet ook de overheid meer verantwoordelijkheid en regie nemen op dit onderwerp. Want de kennis en kunde blijkt in het veld zeker aanwezig, maar de sturing ontbreekt. Digitale veiligheid stevig op de bestuursagenda, structureel samenwerken en kennis actualiseren, en goed sturen op stelselniveau."
- **Ministerie van Onderwijs, Cultuur en Wetenschap**
  "De digitale veiligheid in het primair en voortgezet onderwijs moet naar een hoger niveau. Dat kan alleen met een integrale en overkoepelende aanpak waarbij in de sector en op schoolniveau alle noodzakelijke aandacht is [...]."

Probleemanalyse

- Het is voor schoolbesturen onvoldoende duidelijk wat ‘veilig’ is en wat daarvoor gedaan moet worden
- De consequenties van het niet goed regelen van privacy en beveiliging worden door schoolbesturen onvoldoende gevoeld
- Het is voor individuele schoolbesturen zeer kostbaar en in sommige gevallen moeilijk uitvoerbaar om alle passende maatregelen op het gebied van privacy en cybersecurity te organiseren

Datum
12 januari 2023

Onze referentie
35528954

Handout Sessie 3

Rondetafelbijeenkomst 3: Data delen

Den Bosch | 10 november 2022

AUTORITEIT PERSOONSGEGEVENS

AVG – Wat is belangrijk bij datadeling?

Twee (van de vele) uitgangspunten:

1. Risicogebaseerd
2. Eigen verantwoordelijkheid/accountability

Dit vraagt om beheersing van processen!

'De Autoriteit Persoonsgegevens is de onafhankelijke toezichthouder in Nederland die de bescherming van persoonsgegevens bevordert en bewaakt'

Denk hierbij aan…

- Privacygovernance
  - Rol van de FG en privacyofficers
  - Bestuur
- Documentatie
  - Verwerkersovereenkomsten: wat mag een leverancier wel/niet doen met persoonsgegevens?
  - Risicobeoordelingen/DPIA's: welke privacyrisico's heeft de verwerking en welke maatregelen moet u treffen?
  - Register van verwerkingen: welke verwerkingen van persoonsgegevens vinden er plaats?
- Processen
  - In kaart brengen van 'datastromen': wie krijgt wat? Hoe houd je zicht op nieuwe datastromen?
  - Beschermingsmaatregelen vooraf bepalen, uitvoeren en controleren: wie bepaalt dit? Hoe en wanneer wordt er gecontroleerd? Wie voert dit uit en controleert dit?

Advies AP

- Onderwijsinstellingen actief te informeren over de verantwoordelijkheden die zij hebben bij het bepalen van de risico's voor kinderen indien digitale middelen worden ingezet en het daarbij aanreiken van middelen om onderwijsinstellingen te stimuleren een dergelijke analyse uit te voeren o uit te laten voeren.
- Verkennen welke digitale middelen veel gebruikt worden door onderwijsinstellingen en het daarop laten uitvoeren van - actueel te houden - DPIA's die kunnen worden gebruikt door onderwijsinstellingen bij hun risicoanalyse. Als onderdeel daarvan, wanneer daar aanleiding toe

Casus: digitale leermiddelen

Heeft u in beeld:

- welke digitale leermiddelen er worden gebruikt binnen uw organisatie (incl. apps)? Zo ja;
- welke gegevens van leerlingen/studenten (en personeel) worden gedeeld/verkocht met de leveranciers van deze leermiddelen en wat de privacyrisico's daarbij zijn? Zo ja;
- of u goede afspraken heeft gemaakt met de leveranciers?

gezamenlijk aanbestedingen van veilige software. Hogescholen vermijden schaduwsoftware en kopen hun software in volgens veiligheidsrichtlijnen. Ook

Bekijk ook eens…

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

https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/paper_autoriteit_persoonsgegevens_digitalisering_in_het_onderwijs_2021.pdf

Datum
12 januari 2023

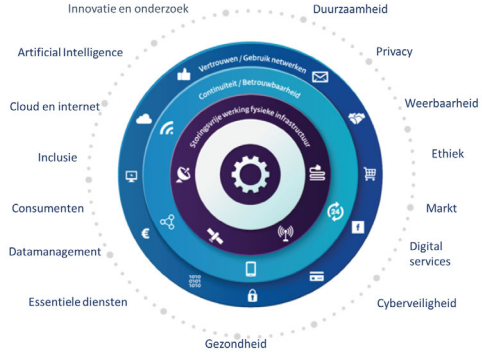
Onze referentie
35528954

Handout Sessie 4

Ketensamenwerking en veiligheid van data

Agentschap Telecom
Ministerie van Economische Zaken en Klimaat

Verschuiving van vraagstukken in het digitaal domein

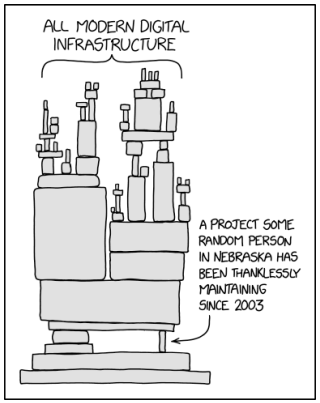


Waarom hebben we het over ketens?

"Een keten is zo sterk als de zwakste schakel"

Digitalisering van ketens
- Steeds meer schakels worden aan een netwerk gekoppeld
- Diensten worden vaker uitbesteed, bijv. aan cloud providers

Ketens doelwit van (gerichte) aanvallen
- Aanvallen op centrale punten in ketens schalen goed
- 'De voordeur' is tegenwoordig steeds beter beveiligd, dus wordt 'de achterdeur' een logisch nieuw doelwit



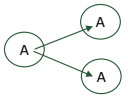
Van keten naar ecosysteem

Supplychain

Productie

Specificaties

Levering

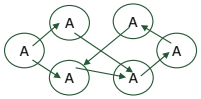


Outsourcing

Competenties

Afbakening taken

Service levels



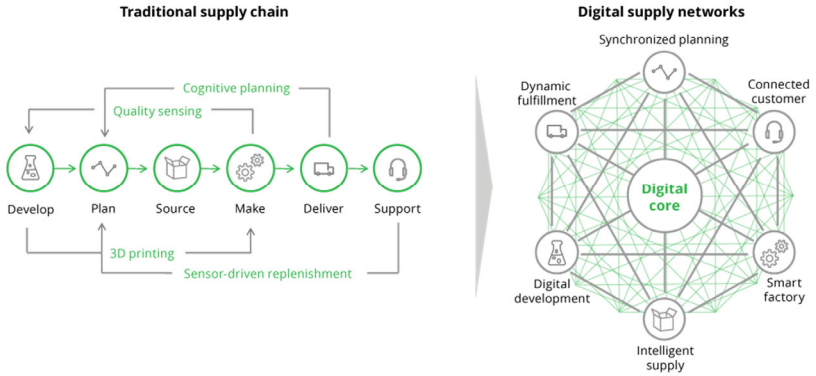
Ecosysteem

Innovatie

Geintegreerde oplossingen

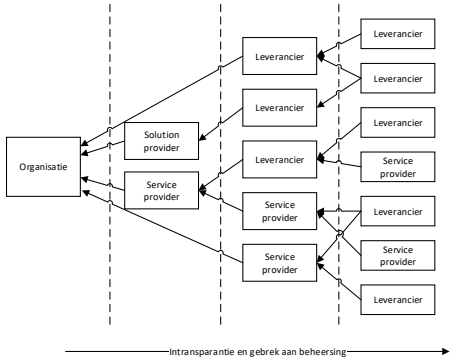
Groei, waarde creatie

Ontwikkelende supply-chains



Complexiteit van ketens

- Risicobeoordeling wordt lastig door intransparante afhankelijkheden in een complexe keten
- Mogelijkheid op controle van de keten neemt af, bijvoorbeeld door globalisering en open-source software



Veelvoorkomend: marktmacht

Voorbeeld: Digitale producten en diensten zijn geconsolideerd in techreuzen.

- (Beveiligings)wensen van individuele afnemers doen er niet toe als niet het merendeel van de afnemers deze wens heeft.
- Afnemers komen vast te zitten in ecosystemen, ook als (enkele) producten in dit ecosysteem niet naar wens zijn.

Incidenten – Vijf beruchte digitale supply chain aanvallen

2013 Target supermarkten in de VS: Inbraak in het netwerk van de supermarktketen Target met behulp van netwerkreferenties die waren gestolen van een leverancier van koelapparatuur.

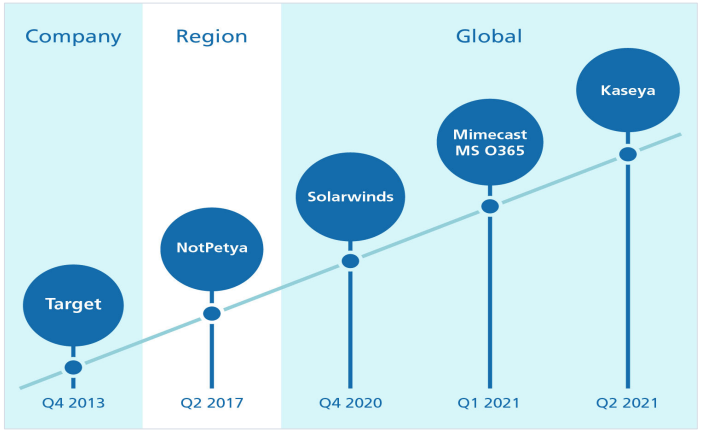
2017 Oekraïne: Regering, financiële instellingen en energiebedrijven in Oekraïne getroffen door de NotPetya-ransomware. Deze aanval was primair gericht op de Oekraïne maar ook bedrijven elders werden getroffen zoals het containervervoerbedrijf Maersk. De Oekraïense boekhoudsoftware MeDoc, werd gecompromitteerd en gebruikt om ransomware te downloaden en uit te voeren in plaats van software updates.

2020 SolarWinds: Duizenden organisaties bleken slachtoffer te zijn van een supply chain aanval via de software van SolarWinds. Dit bedrijf levert software voor het monitoren van IT-omgevingen. Aanvallers wisten via een backdoor updates aan Solarwinds-software toe te voegen, waardoor ze toegang kregen tot de systemen van de getroffen organisaties.

2021 Mimecast/MS 365: Een certificaat van e-mailbeveiligingsbedrijf Mimecast was gecompromitteerd en werd door aanvallers gebruikt om toegang tot Microsoft 365-accounts van klanten te krijgen. Het door Mimecast uitgegeven certificaat wordt door bedrijven gebruikt om een beveiligde verbinding tussen de Mimecast-diensten en Microsoft 365 Exchange tot stand te brengen.

2021 Kaseya: Dit tool dat gebruikt wordt om software op afstand te beheren werd gehackt, waardoor hackers via Kaseya bedrijven wisten te infecteren met malware. Niet alleen directe klanten van Kaseya werden getroffen, ook klanten van die klanten. Daarmee is een domino-effect ontstaan dat nooit eerder was gezien.

Incidenten – Steeds grotere reikwijdte



Ketenrisico's - inzicht krijgen in afhankelijkheden en dreigingen

- Een manier om dreigingen door concentratie op een locatie en afhankelijkheden van een leverancier in kaart te brengen is via het OSI-model.
- Dit model geeft de relaties weer vanuit het perspectief van datatransport en verbindingen. Hierdoor ontstaat een totaaloverzicht van zowel de afzonderlijke leveranciers als de samenhang tussen hun toeleveranciers.
- Voor de dreiging door aanvallen via (toe)leveranciers dient gekeken te worden of diensten dan wel software van een leverancier op veel plekken of processen binnen een bedrijf voorkomen. Ook is het zaak na te gaan of ze toegang bieden tot belangrijke bedrijfsprocessen of informatie.