Digitaal Veilig Onderwijs WMS congres

Marloes Kotkamp

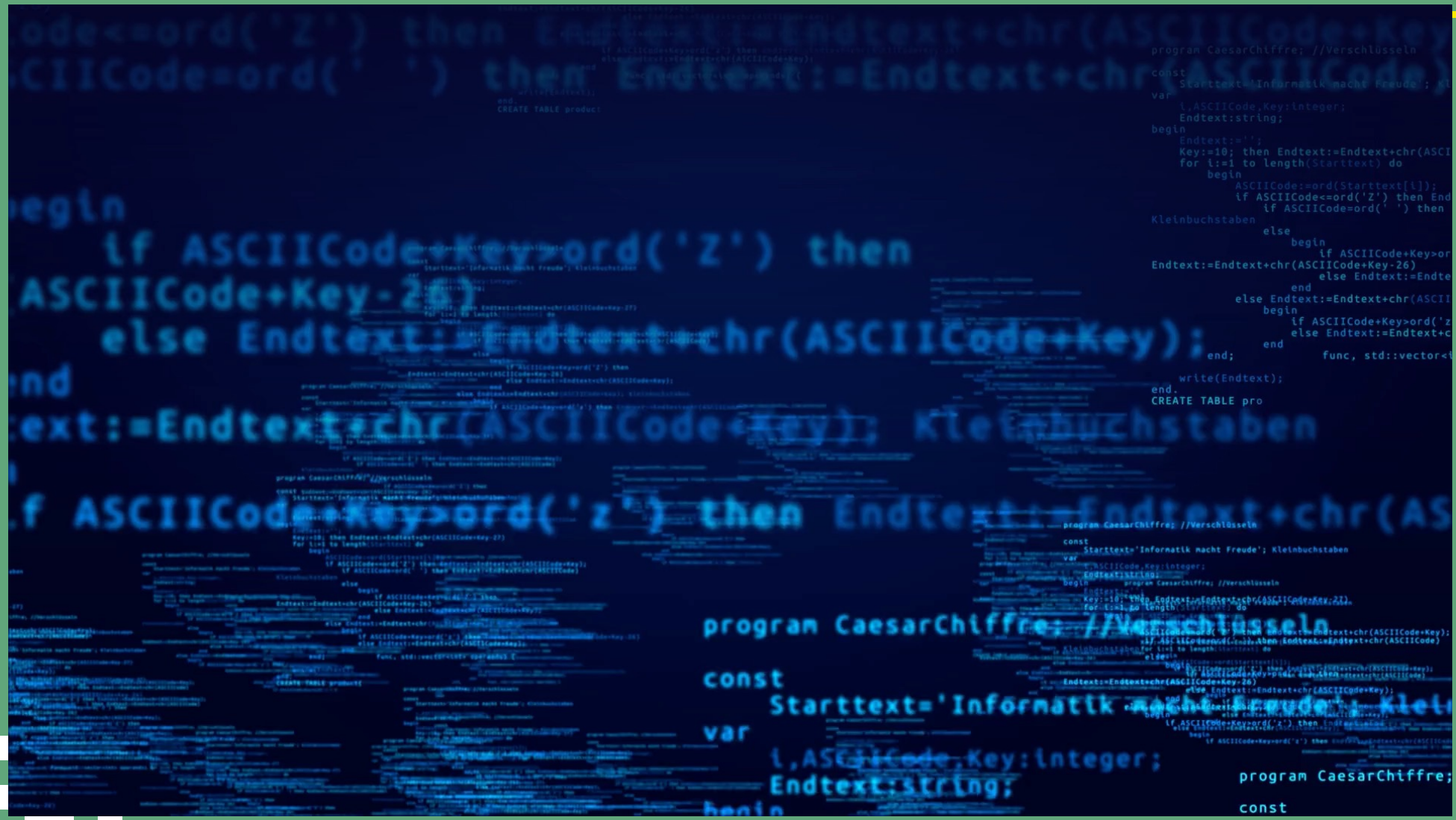
19 november 2025

Bit by Bit
Samen voor digitaal veilig onderwijs

PO RAAD VO RAAD

Marloes Kotkamp

- ❑ Projectmedewerker PO-Raad/ VO-raad
- ❑ Per 1 december nieuwe baan in de cybersecurity voor schoolbesturen en samenwerkingsverbanden
- ❑ Boss Lady in de overhemden business



Bit by Bit

Samen voor digitaal veilig onderwijs

PO RAAD VO RAAD

Is jullie school goed voorbereid op een (cyber)incident?

Bit by Bit
Samen voor digitaal veilig onderwijs

PO RAAD VO RAAD

Digitaal Veilig Onderwijs

- Programma Digitaal Veilig Onderwijs (programma DVO)
- Nulmeting (2023)
- De Raden richten zich op: bewustwording, activering en professionalisering.
- Kennisnet: Normenkader IBP | 69 normen IB en 25 voor privacy
- SIVON: Deep Dive Workshops Deep Dive Workshops - SIVON
- School-CERT | AANMELDEN!! School-CERT - Kennisnet

➢ Zelfevaluatie van het Normenkader IBP Wijzer Platform

PO RAAD VO RAAD

Concreet

Ministerie van Onderwijs, Cultuur en Wetenschap

Nieuwsbrieven Ministerie van OCW > Actueel > Nieuws

Digitaal veilig onderwijs vraagt nu actie van schoolbesturen

Nieuwsbericht | 13-11-2025 | 17:40

Schoolbesturen en het ministerie van OCW hebben afgesproken dat scholen vanaf 2030 voldoen aan landelijke normen voor een digitaal veilige schoolomgeving. Vanaf 1 januari 2027 moeten scholen weten waar ze staan ten opzichte van deze normen door een zelfevaluatie uit te voeren. Ook moet er dan een plan zijn om aan alle normen te voldoen. Want alle leerlingen en medewerkers in het funderend onderwijs hebben recht op een digitaal veilige leer- en werkomgeving.

Cyberdreigingen nemen toe

Het Dreigingsbeeld Cybersecurity 2025 van Kennisnet laat zien dat het aantal cyberaanvallen in het primair en voortgezet onderwijs sinds 2023 is toegenomen. Het uitvoeren van cyberaanvallen wordt steeds eenvoudiger en goedkoper terwijl deze aanvallen tegelijkertijd moeilijker te herkennen zijn. Steeds vaker gaat het (bijna) mis, waardoor gegevens op straat komen te liggen of lessen niet kunnen doorgaan.

- Scholen moeten vóór 1 januari 2027 weten waar ze staan rondom DVO.
- Wijzer Platform

- Per 2030 moeten alle scholen in het funderend onderwijs voldoen aan de landelijke norm.

Digitaal veilig onderwijs vraagt nu actie van schoolbesturen | Nieuwsbrieven Ministerie van OCW

PO RAAD VO RAAD

- IBP is geen ICT-feestje

Bit by Bit
Samen voor digitaal veilig onderwijs

PO RAAD VO RAAD

Bit by Bit
Samen voor digitaal veilig onderwijs

In 2025 vonden in Nederland meerdere digitale aanvallen plaats die impact hadden op schoolprocessen en bedrijfsvoering, met onder andere tot gevolg:

- verstoring van het onderwijs;
- leveringsvertraging van bestellingen en uitgevallen schoolexamens door cyberincidenten bij leveranciers;
- frauduleuze bestellingen uit naam van schoolbesturen;
- misbruik van ICT-middelen;
- afhandig maken van inloggegevens.

Bron: Kennisnet 2025

[Dreigingsbeeld Funderend Onderwijs]

PO RAAD VO RAAD

GEVOLGEN VAN EEN INCIDENT

DATALEK

- Verlies van betrouwbaarheid, intern en extern
- Juridische claims van betrokkenen
- Imagoschade voor de organisatie

DDOS

- Geen toegang tot betalingen, deadlines en declaraties worden gemist.
- Productiviteitsverlies, alles ligt stil.
- Schade heeft vaak hoge kosten.

RANSOMWARE

- Geen toegang tot financiële systemen bijv. AFAS of Exact.
- Grote operationele gevolgen om de impact op te lossen.
- Schade heeft vaak hoge kosten.
- Je kan nergens meer bij, alles is versleuteld

IDENTITEITSFRAUDE

- Jouw gegevens worden door criminelen gebruikt voor aankopen online.
- Schulden op jouw naam

Bit by Bit

Samen voor digitaal veilig onderwijs

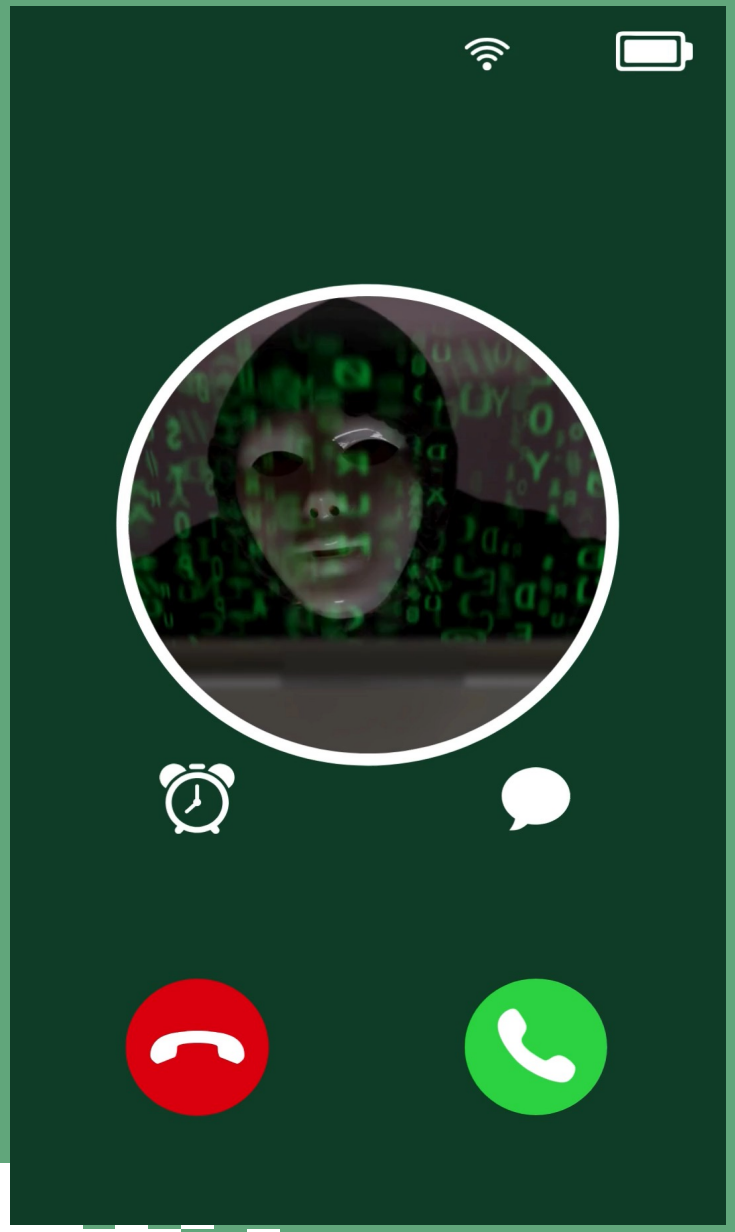
PO RAAD VO RAAD

Ondersteuningsaanbod project VDD

- Leertraject ‘Regie op Digitalisering’
- Handreiking bestuursverslag.
- Handreiking 'Sturen op digitale veiligheid’
- Handreiking 'De rol van de RvT’
- Masterclasses en Webinars voor schoolleiders, leden RvT en éénpitters.
- Ondersteuning Samenwerkingsverbanden
- Kennisoverdracht bij Kennisgroepen binnen de Raden

Aankomende evenementen

- Nog twee Deep Dive Workshops in 2025 | SIVON
- 5-daagse voor kleine schoolbesturen 2026 | SIVON
- NOZON training 2026 | Kennisnet



Ga met je bestuurder(s) in gesprek over de stappen die zij willen zetten in Q1 2026 in het kader van Digitaal Veilig Onderwijs.

Vragen aan je bestuurder(s)

- Welke stappen gaat het bestuur in het eerste kwartaal van 2026 zetten om de digitale veilgheid van onze school/ scholen te verbeteren
- Hoe worden medewerkers en leerlingen betrokken bij het veiliger maken van onze digitale omgeving?
- Wat doet het bestuur om te voorkomen dat er gevoelige informatie (zoals leerlinggegevens) in verkeerde handen valt?
- Hoe wordt er samengewerkt met externe partijen, zoals de politie of IT-dienstverleners , om digitale risico's te beperken?
- Hoe worden wij als (G)MR op de hoogte gehouden van incidenten of verbeteracties op het gebied van digitale veiligheid?

Bit by Bit
Samen voor digitaal veilig onderwijs

PO RAAD VO RAAD

Vragen of hulp?

Gabriëlle Putuhena

gabriëlleputuhena@vo-raad.nl

Marloes Kotkamp

m.kotkamp@poraad.nl

Let op tot 1 december 2025

of digitalisering@povosi.nl

SAMEN STERKER TEGEN ONLINE DREIGINGEN

WMS congres 19 november 2025

Onno Sidler

Accountmanager Cybercrime Publiek Private Samenwerking

Team Cybercrime Oost-Brabant

POLITIE

Waar gaan we het over hebben?

- Wat weten jullie al van cybercrime?
- Hoe komen leerlingen in aanraking met (online) criminaliteit?
- Met welke cyberdreigingen heeft een school te maken?
- Daderschap bij leerlingen, wat kan jij doen?
- Hands on: aan de slag met een casus

POLITIE

Weten jullie wat wel en niet mag?

POLITIE

Situatie 1:

De docent vergeet zijn scherm te vergrendelen als hij koffie gaat halen. Jij loopt langs het scherm en ziet de leerlingkaart van Jeffrey openstaan met een 4,5 voor biologie. Je vertelt meteen aan de hele klas dat Jeffrey een dikke onvoldoende heeft gescoord.

POLITIE

Situatie 1a:

De docent vergeet zijn scherm te vergrendelen als hij koffie gaat halen. Jij ziet de leerlingkaart van Jeffrey openstaan en je weet dat jij erna komt in de lijst. Je klikt 1 kaart verder en je ziet jouw resultaten.

Wetboek van strafrecht:
138ab – computervredebreuk

1. *Met gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie wordt, als schuldig aan computervredebreuk, gestraft hij die opzettelijk en wederrechtelijk binnendringt in een geautomatiseerd werk of in een deel daarvan. (...)*

POLITIE

Computervredebreuk in real life

POLITIE

Situatie 2:

De wifi op school is supertraag, maar gelukkig kan je het snellere wifi-netwerk van de docenten ook ontvangen. Omdat het wachtwoord voor docenten al jarenlang “D0c3nt-2019” is kan je gewoon inloggen op deze wifi.

Wetboek van strafrecht:
138ab lid 1 – computervredebreuk

1. *Met gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie wordt, als schuldig aan computervredebreuk, gestraft hij die opzettelijk en wederrechtelijk binnendringt in een geautomatiseerd werk of in een deel daarvan. Van binnendringen is in ieder geval sprake indien de toegang tot het werk wordt verworven:*
   - *met behulp van valse signalen of een valse sleutel,*

POLITIE

Computervredebreuk met een valse sleutel in real life

POLITIE

Situatie 3:

Je vriend Thomas is even weg en heeft zijn telefoon laten liggen. Je weet zijn code en na het inloggen kom je meteen in zijn fotoalbum. Je ziet een foto van hem in een belachelijke outfit en je besluit die foto naar jezelf door te appen. Altijd leuk voor later om hem nog eens mee te confronteren ;-)

Wetboek van strafrecht:
138ab lid 2 – computervredebreuk, strafverzwaring

2. *Met gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie wordt gestraft computervredebreuk, indien de dader vervolgens gegevens die zijn opgeslagen, worden verwerkt of overgedragen door middel van het geautomatiseerd werk waarin hij zich wederrechtelijk bevindt,* ***voor zichzelf of een ander overneemt, aftapt of opneemt****.*

POLITIE

Computervredebreuk met diefstal voor eigen gewin in real life

Insluiping en diefstal Apple laptops uit het Kaj Munk college

HOOFDDORP 28-01-2014, 21:31 **Gewijzigd:** 11-04-2014, 16:05

De dader zeult de dure Macbooks in twee tassen naar buiten.

Situatie 4:

Sabine heeft het uitgemaakt met Jaap en Jaap besluit als wraak een deepfake-sexfilmpje van Sabine te maken.

Wetboek van strafrecht:
245BA

- Met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie wordt gestraft:
- a. hij die opzettelijk en wederrechtelijk van een persoon een visuele weergave van seksuele aard vervaardigt;

POLITIE

Situatie 4a:

Jaap heeft het deepfake sexfilmpje van Sabine doorgestuurd naar Bas. Bas vindt het erg grappig en bewaart het filmpje in zijn camerarol. Is Bas dan ook strafbaar?

Wetboek van strafrecht:
245BA

- Met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie wordt gestraft:
- a. hij die opzettelijk en wederrechtelijk van een persoon een visuele weergave van seksuele aard vervaardigt;
- b. hij die de beschikking heeft over een visuele weergave als bedoeld onder a terwijl hij weet of redelijkerwijs moet vermoeden dat deze door of als gevolg van een onder a strafbaar gestelde handeling is verkregen.

POLITIE

Situatie 5:

Je vindt de docent Duits, Dhr. Cees Scheele, veel te streng en je roept op TikTok iedereen op om in de Plutoniumstraat nummer 4 langs te rijden en te toeteren en dan te roepen “Wat kan ons het nou schelen Kees!” Best grappig vind jij want hij kijkt ook een beetje scheel. Mag dit?

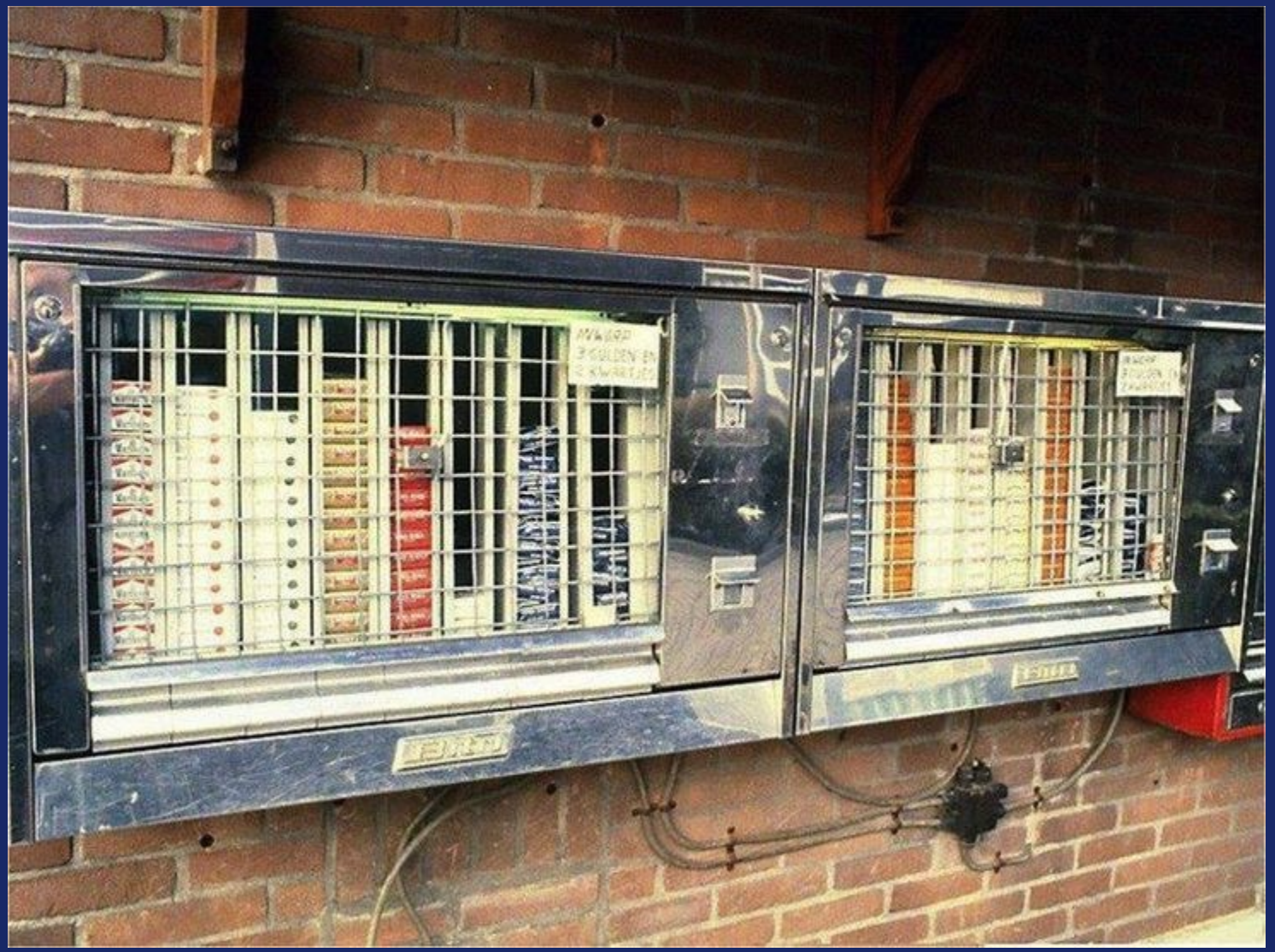
Wetboek van strafrecht:
285d

- Degene die zich persoonsgegevens van een ander of een derde verschaft, deze gegevens verspreidt of anderszins ter beschikking stelt met het oogmerk om die ander vrees aan te jagen dan wel aan te laten jagen, ernstige overlast aan te doen dan wel aan te laten doen of hem in de uitoefening van zijn ambt of beroep ernstig te hinderen dan wel ernstig te laten hinderen, wordt gestraft met gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie.

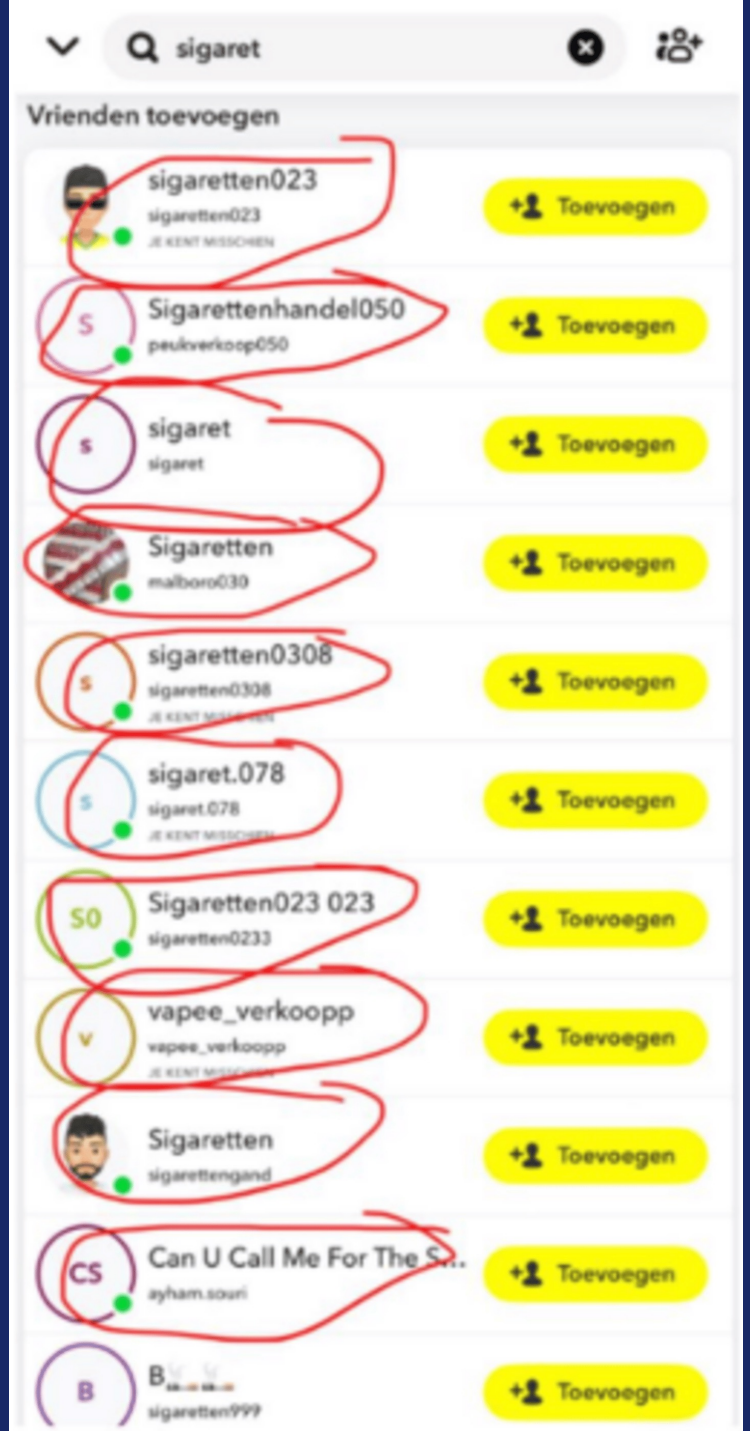
POLITIE

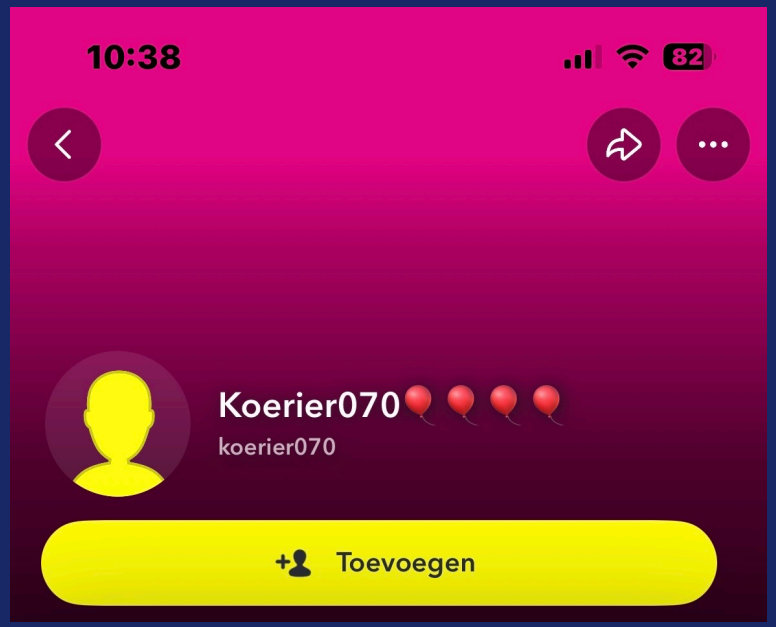
Hoe komen onze leerlingen in aanraking met (online) criminaliteit?

POLITIE



POLITIE





Algemene druggerelateerde symbolen

- 🍁: Een universeel symbool voor drugs in het algemeen, of specifiek voor cannabis.
- 💊: Algemeen symbool voor pillen, medicatie, maar vaak in druggerelateerde context voor XTC, MDMA, of (namaak)pillen op voorschrift.
- 🔪:Een dealer, iemand die je kan "regelen" (hook you up).
- 🤑/💰/🏧/💳 : Worden gebruikt om te adverteren dat iemand drugs verkoopt, of als signalen van een 'succesvolle' dealer.
- 📦 / ◻: Voor het bespreken van verzending of levering van drugs.
- 📱/📲: Kan duiden op de bereidheid van dealers om te leveren.
- 🍪 / 🍯: Grote hoeveelheid drugs, een 'batch'.
- 🚀 / 💥 / 💣: Duiden op hoge potentie van de drugs, of de effecten van het gebruik (bijv. "Ik ben 🚀").

Specifieke drugs en gerelateerde effecten

Cannabis (Wiet, Hasj)

- 🌿 / 🍃/ 🌳 / 🌴 / 🎄 / 🍀 / 🌳: Allemaal symbolen voor wiet/marihuana.
- 🫁 / 🔥: Roken, blowen, of 'stoned' zijn.
- 🚬: Kan een joint symboliseren.
- ◻: Kan een joint vasthouden.
- ⏰: "Tijd om stoned te worden."
- 👽 / 🫧 / 😁 / 😅 / 😵‍💫 / 😶: Gevoelens van "high" zijn, veranderd bewustzijn, of geheimhouding.

Cocaïne

- ❄️ / 🌨 / ☃️: Symbolen voor cocaïne ("sneeuw").
- 🎱: Specifiek voor cocaïne.
- 🔑: Kan verwijzen naar "key" of een 'key bump' (kleine hoeveelheid cocaïne).
- 🥥: Kan verwijzen naar cocaïne.
- 👃 (of 🤧): Voor snuiven.
- 💎: Ook voor cocaïne, of methamfetamine ("crystal").
- 🐵: Kan ook voor cocaïne worden gebruikt.

MDMA / XTC / Molly

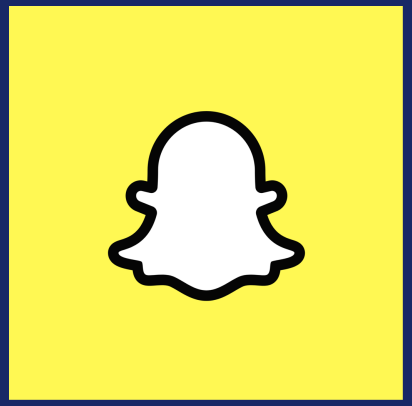
- ❤️ / 💜: Voor de 'liefdevolle' effecten van MDMA.
- 💊: MDMA-pillen of 'candy-flipping' (MDMA en LSD).
- ⚡: Kan de energie of de "inslag" van MDMA symboliseren.
- 🤯: De intense ervaring.

Paddo's / Psychedelica

- 🍄: Voor paddo's of andere hallucinogene paddenstoelen.
- 🌈 / ✨: Kan verwijzen naar psychedelische ervaringen.

Op welke platformen komen leerlingen in aanraking met online criminaliteit?

- Scammers (Ruilen gekochte items / misleidende links)
- Grooming
- Malware / virussen
- Diefstal Robux
- Account takeover
- Cyberpesten
- Ongepaste inhoud

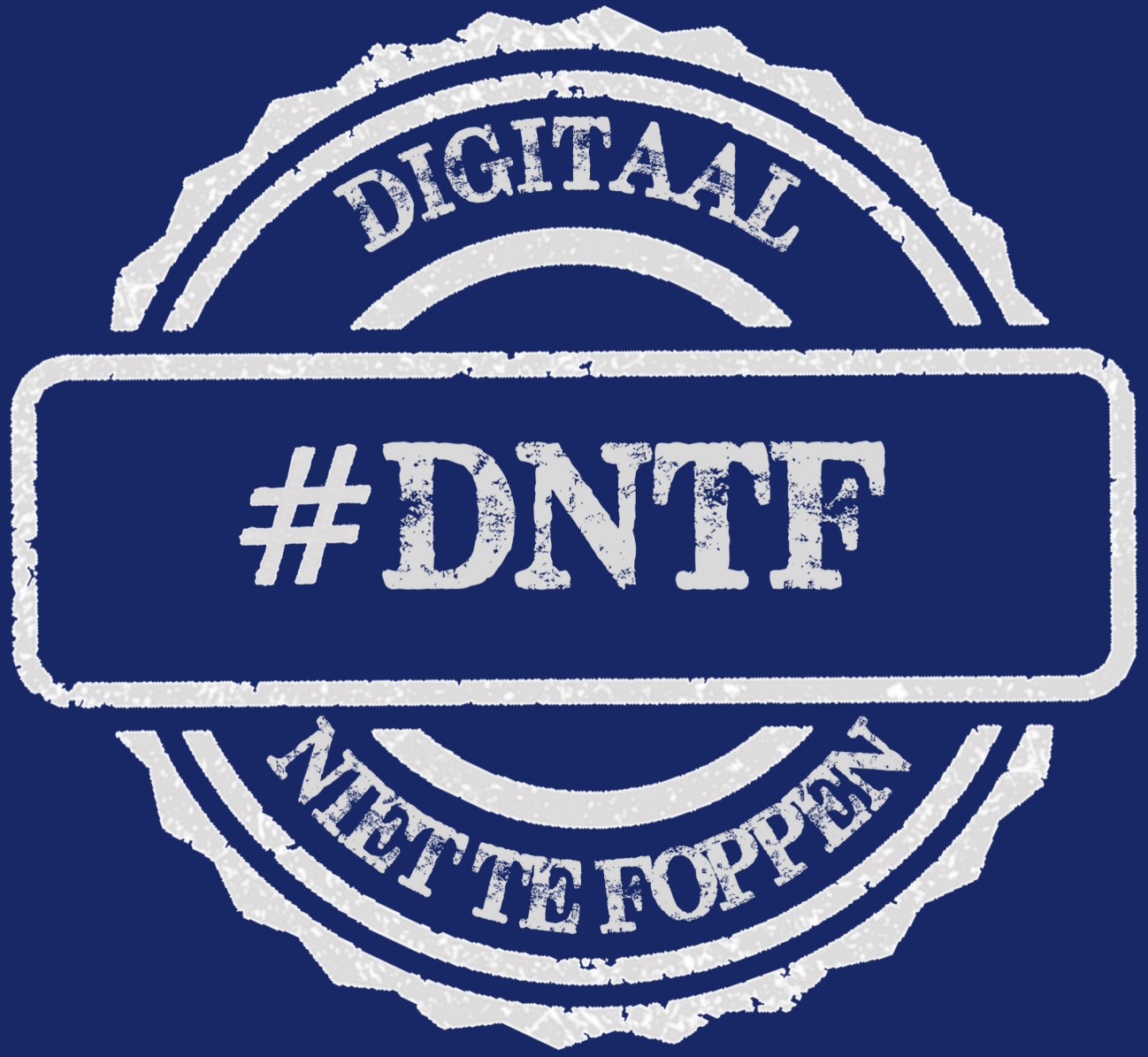


- Contact met kwaadwillenden
- Ongepaste inhoud
- Verkoop illegale middelen
- Pesten en intimidatie
- Dealers voor sigaretten, snus, drugs, vapes, vuurwerk

- Wapenhandel en explosieven
- Vuurwerk
- Kinderporno
- Ronselen
- Voorbereiden aanslagen

- Contact met kwaadwillenden
- Ongepaste inhoud
- Grooming
- Pesten en intimidatie

POLITIE



POLITIE

Aanleiding

Vanuit de themasessie cybercrime en onderwijs op 8 juni 2023:

“Scholen vinden het lastig om cybercrime te integreren als thema binnen het curriculum”

Hoe gaan we om met:

- *De school als slachtoffer van een cyberaanval*
- *Daderschap bij leerlingen*
- ➢ ***Slachtofferschap bij docenten en leerlingen***

Er is behoefte aan:

- *Beleid omtrent cybercrime in relatie tot de school*
- ➢ ***Vergroten van de cyberweerbaarheid bij docenten en leerlingen***

POLITIE

De hoeveelheid aandacht voor digitale geletterdheid in de lessen verschilt per onderwerp

po	aandacht	vo
• zoeken en vinden van betrouwbare informatie op internet	**meest**	• betrouwbare informatie zoeken op internet
• tekstverwerken en gebruik van presentatie-programma’s • online pesten • sociale media • nepnieuws/fake news • online veiligheid en privacy	**veel**	• Office-toepassingen als Word, Excel en PowerPoint • nepnieuws/fake news • beeldtaal (informatie in de vorm van beeld i.p.v. tekst) • sociale media
• journalistiek • cybercrime • technologische innovaties/techniek en toekomst	**minst**	• cybercrime • programmeren • digitale marketing/ online marketing
	meest tijdens mentor uren:	• gebruik van mobiele telefoon op school • inzet van afstands-onderwijs • online pesten • WhatsApp-gebruik

Bron: Factsheet digitale geletterdheid – SLO september 2023

Het doel:

Jaarlijks terugkerende aandacht voor digitale criminaliteit in het curriculum PO-VO om de cyberweerbaarheid onder leerlingen te vergroten

POLITIE

Het project

- PO en VO pilot scholen
- Trainen docenten
- Lessen gegeven door docenten
- Onderzoek UvU cyberbewustzijn
- Onderzoek Avans behoefte docenten
- Onderzoek Avans leeropbrengst politie
- Blauwdruk visiedocument Edux
- Opschaling PO-VO raad, Kennisnet, expertisepunt DG, Impuls open leermateriaal, Bibliotheek Eindhoven

POLITIE

Opgeleverde documenten:

Blauwdruk visie document

Onderzoek cyberbewustzijn bij leerlingen

Utrecht University

Onderzoek Behoeftes van Docenten mbt implementatie

avans

Onderzoek rendement gastles politie

avans

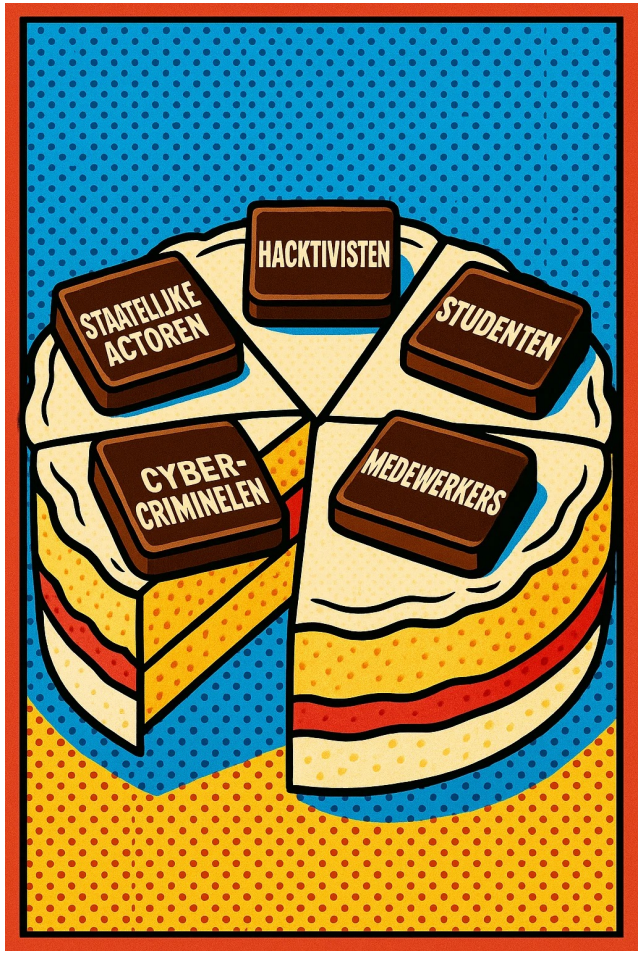
POLITIE

https://www.wikiwijs.nl/startpagina/cybercrime

Met welke cyberdreigingen heeft de school te maken?

POLITIE

Met welke actoren heeft een school te maken?



Statelijke actoren:
- Spionage
- Economische of politieke voordelen
- Politieke doelstellingen bereiken
- Ontwrichting

Studenten:
- Persoonlijk voordeel (bv inzicht)
- Verstoring (bv uitstel examen)
- Doxing

Studenten - Cyberbreinen:
- Nieuwsgierigheid
- (responsible?) disclosure

Cybercriminelen:
- Geldelijk gewin
- Profilering van de groep

Hacktivisten:
- Aandacht voor hun standpunt

Medewerkers:
- Onwetendheid
- Onachtzaamheid
- Gemak
- Gebrek aan cyberbewustzijn

POLITIE

En wat doen jullie als een leerling de fout in gaat?

POLITIE

Wat betekent aangifte voor de toekomst van de leerling?

- Aantekening / strafblad?
  - Vanaf 12 jaar
  - Overtreding heeft 5 jaar bewaartermijn
  - Misdrijf heeft 20 jaar bewaartermijn + tijd van eventuele gevangenisstraf
  - VOG (tot 23 jaar) – Men kijkt of je afgelopen 2 jaar iets of je strafblad hebt gekregen
- Stopgesprek – eenmalig geen strafblad (afhankelijk van ernst en gevolgen)
- Alternatieve interventie – Hackright (uitspraak door officier – strafblad?)

POLITIE

Wat kan je als school zelf doen?

- In afstemming met leerling en ouders een alternatieve afdoening afspreken (afhankelijk van de ernst en de schade)
  - In gesprek met de ICT-er zicht krijgen op de schade die je de school en/of personen hebt aangericht en afspraken maken over hoe dit op te lossen
  - In een individueel traject een lesprogramma als Cyberethiek volgen
  - Afhankelijk van de situatie afspraken maken over responsible disclosure taken voor de leerling

POLITIE

Waar kan je terecht voor hulp?

Stichting Cyberbrein	https://cyberbrein.nl/
DIVD	https://www.divd.nl/
Politie	Onno Sidler - onno.sidler@politie.nl

POLITIE

Handen uit de mouwen:
Hoe bereiden wij ons voor op cyberdreigingen?

POLITIE

Cyberincident: Ransomware

Het is zondagavond 19.00 uur als het hoofd ICT van de school contact opneemt met de directie. De school is slachtoffer geworden van een Ransomware aanval. In een ransomnote is aangegeven dat de daders 1,1 bitcoin eisen binnen een week te betalen. Als de school niet betaalt blijven de bestanden versleuteld en zullen de daders via een leakpage de data van de school te koop aanbieden op het darkweb. Om te laten zien dat ze het menen is er nu al een kleine greep uit de schoolbestanden op de leakpage gezet. Hier zien we een paar facturen van het cateringberdijf aan de school en een boekje van de schoolreis naar Praag van afgelopen jaar.

Alle bestanden binnen de schoolomgeving zijn versleuteld en niet meer te openen. Ook zijn belangrijke administratieve programma's niet meer toegankelijk zoals het personeelssysteem, het leerlingvolgsysteem en de mail.

De ICT afdeling geeft aan nog geen idee van de impact en de omvang te hebben. Wel is duidelijk dat bepaalde systeemaccounts zijn overgenomen. Maar hoe lang de daders al in de omgeving zijn, waar ze toegang toe hebben gehad en welke informatie gelekt kan zijn is niet duidelijk.

Opdracht:
Aan jullie nu de vraag:

- Welke beslissingen de school gaat nemen, (onder andere of je gaat betalen of niet)
- Wie je erbij gaat betrekken, (incident response? En wie dan? AP? En wat ga je dan vertellen? Of doe je dat later?)
- Wat je hierover gaat communiceren en aan wie? En wanneer ga je communiceren? En via welk medium?
- Informeer je meteen de politie? En ben je bereid aangifte te doen? En wat betekent aangifte doen voor jullie?

Noteer ook alle vragen die in jullie groepje naar boven komen en waar je eigenlijk nog geen antwoord op hebt.

POLITIE

Cyberincident: DDOS

Het is de tentamenweek op het Jan van Stramman College. Vandaag staat het examen natuurkunde en wiskunde op het programma. Maar vlak voor het examen wiskunde dat landelijk op een vast tijdstip begint lopen alle computersystemen op school vast. De school ligt onder een DDOS aanval. Bij vlagen is er af en toe weer een klein beetje verbinding maar het examensysteem ligt plat en het examen wiskunde kan niet doorgaan. De vraag is of Natuurkunde dat drie uur later begint wel door kan gaan.

De ICT afdeling krijgt er nog geen grip op wie er achter de aanval zit, maar alles wijst erop dat het signaal uit het netwerk van de school zelf komt en dat het waarschijnlijk een leerling is die hierachter zit.

Binnen het bestuur zitten nog twee andere scholen die door de DDOS ook plat liggen en dus ook geen examen wiskunde kunnen maken. Als de school snel schakelt kunnen ze gebruik maken van de wasstraat van een incident response bedrijf die ervoor kunnen zorgen dat de DDOS aanval van de andere twee scholen wordt weggeleid zodat het natuurkunde examen daar wel door kan gaan. Dit is echter een prijzige exercitie die minimaal €15.000 gaat kosten.

Tot slot zijn er ook al ouders die er via hun kind lucht van hebben gekregen en bang zijn dat hun zoon of dochter nu in de vakantie herexamen moet doen. Ze dreigen al met een claim voor de kosten van een misgelopen vakantie.

Opdracht:
Aan jullie nu de vraag:
Welke beslissingen de school gaat nemen, (gaan we de DDOS wasstraat inzetten? Hebben we genoeg juridische kennis om op de claim van de ouders te reageren?)
Wie je erbij gaat betrekken, (incident response? En wie dan? AP? Is dat nodig?)
Wat je hierover gaat communiceren en aan wie? En wanneer ga je communiceren? En via welk medium?
Informeer je meteen de politie? En ben je bereid aangifte te doen? En wat betekent aangifte doen voor jullie? En wat betekent dit eventueel voor een leerling die hierachter kan zitten?
Als hier een leerling achter zit, wat doe je daar dan mee? Wordt hij geschorst? Van school gestuurd? Ga je een begeleidingsprogramma voor hem opzetten en hoe doe je dat dan?

Noteer ook alle vragen die in jullie groepje naar boven komen en waar je eigenlijk nog geen antwoord op hebt.

POLITIE

Cyberincident M365

In de coronatijd hebben we Microsoft Teams aangezet om online lessen te kunnen geven en nadien werd dit zoveel gebruikt dat we het open hebben laten staan. En daar plukken we nu de zure vruchten van.
Medewerkers konden zelf teams aanmaken en daar is dankbaar gebruik van gemaakt. Maar een IB-er heeft een team aangemaakt voor hem zelf en een collega en heeft er geen erg in gehad dat het een openbaar team is geworden waar iedereen die het team vindt zichzelf kan inschrijven in dit team. En helaas heeft deze IB-er met de beste bedoelingen exports uit Magister gehaald en in dit team gezet om met zijn collega IB-er de leerlingbesprekingen voor te bereiden.

Een journalist van het plaatselijke dagblad heeft er op een of andere manier lucht van gekregen dat dit team openbaar beschikbaar binnen de organisatie is, en via het account van zijn dochter die ook op jullie school zit heeft hij zich ingeschreven en rondgekeken in dit team. Het zal je niet verbazen dat de volgende dag een smeuïg artikel in de krant staat waarin wordt gezegd dat alle leerlingengegevens van de school open en bloot op straat liggen.

Ouders bellen bezorgd de school op om opheldering te vragen en sommigen dreigen al met een claim richting de school.

De ICT-er van de school geeft aan dat er momenteel 1934 Teams actief zijn in de schoolomgeving waarvan er 29 openbaar zijn. Er zijn momenteel 78 Teams die voor de lessen worden gebruikt en zo'n 57 Teams die door docenten onderling worden gebruikt. Van de overige teams weet men niet waar ze voor zijn, wie erin zit en welke materialen (al dan niet met gevoelige gegeven) erin staan.

Opdracht:
Aan jullie nu de vraag:
Welke beslissingen de school gaat nemen, (Wat doen we nu direct met de Teams omgeving? En welke vervolgacties moeten we hiervoor uitzetten? Hoe garanderen we dat dit niet nog eens kan gebeuren? Hebben we genoeg juridische kennis om op de claim van de ouders te reageren?)
Wie je erbij gaat betrekken, (AP? Is dat nodig? En wanneer gaan we die betrekken? Heeft de school genoeg kennis om het gat nu meteen te dichten?)
Wat je hierover gaat communiceren en aan wie? En wanneer ga je communiceren? En via welk medium?

Noteer ook alle vragen die in jullie groepje naar boven komen en waar je eigenlijk nog geen antwoord op hebt.

POLITIE

Dank voor jullie bijdrage!

Onno Sidler

Accountmanager Cybercrime Publiek Private Samenwerking

Team Cybercrime Oost-Brabant

onno.sidler@politie.nl