Digitaal Veilig Onderwijs

Bit by Bit
Samen voor digitaal veilig onderwijs

Workshop: *'Impact van een cyberincident op de leerling'*

Noëlle Steeghs: beleidsadviseur PO-Raad en VO-raad

Andrea Tegel: communicatieadviseur PO-Raad en VO-raad

PO RAAD VO RAAD

Agenda

- Digitaal Veilig Onderwijs (5 min)
- Dreigingsbeeld po & vo (10 min)
- Aan de slag... (60 min)
- Afsluiting (5 min)

Digitaal Veilig Onderwijs

- **Programma** Digitaal Veilig Onderwijs (programma DVO). Partners: *OCW (opdrachtgever), Kennisnet, SIVON, de PO-Raad en de VO-raad.*
- Belangrijkste programmadoel > In 2027 is het funderend onderwijs digitaal veilig. Schoolbesturen gebruiken het **Normenkader Informatiebeveiliging en Privacy Funderend Onderwijs** als leidraad.
- De PO-Raad en VO-raad richten zich op **bewustwording** en **professionalisering** van *schoolleiders en schoolbestuurders* op het gebied van digitale veiligheid.

Ondersteuningsaanbod

- Leidraad: het Normenkader Informatiebeveiliging en Privacy voor Funderend onderwijs
- 11 basismaatregelen voor informatiebeveiliging
- Aansluiten bij het Netwerk IBP (Informatiebeveiliging en Privacy)
- Dienst Verwerkersovereenkomsten
- Toets Verwerkersovereenkomsten
- Uitvoering van DPIA's (toets op privacyrisico's)

… en meer

www.digitaalveiligonderwijs.nl

Ondersteuningsaanbod

- **Webinar** ***Digitale Veiligheid*** **(voor leden Raden van Toezicht)**

- **datum:** 23 april, 16:00-16:45
- Informatie en aanmelden

- **Leertraject** ***Regie op Digitalisering***

- **start op:** 19 en 20 september ’24
- Informatie en aanmelden: vo-academie.nl

Dreigingsbeeld

- Hoe hebben we het Dreigingsbeeld FO gemaakt?
- Wat zijn de belangrijkste dreigingen voor het onderwijs?
- Wat kun je met het dreigingsbeeld?

PO RAAD VO RAAD

Hoe is het dreigingsbeeld gemaakt?

- Incidenten uit het onderwijs en andere sectoren
- Verschillende bronnen:
  - Dreigingsbeelden uit andere sectoren
  - Internationale bronnen
- Feedback van Klankbordgroep IBP (Informatiebeveiliging en Privacy)
- 1e versie. In de toekomst: meer input vanuit het onderwijs, denk aan het CERT en ervaringsdeskundigen aan het woord.

PO RAAD VO RAAD

Belangrijkste dreigingen zijn:

- Datalekken
- DDoS-aanvallen
- Ransomware
- Afhankelijkheid leveranciers en clouddiensten
- Identiteitsfraude en manipulatie van data

PO RAAD VO RAAD

Dreiging 1: Datalekken

- Verlies of ongeautoriseerde verwerking van persoonsgegevens
- Door cyberincidenten of door onbekwaam gedrag van medewerkers

Voorbeelden: *publicatie van vertrouwelijke informatie van leerlingen en medewerkers op sociale media,* of: *vertrouwelijk zorgdossier wordt naar verkeerde ouders gemaild*

PO RAAD VO RAAD

Dreiging 2: Ransomware

- Gijzelsoftware, losgeld voor vrijgeven systemen of niet lekken van data
- Door ransomware-as-a-service zeer relevant bij lage digitale weerbaarheid

Voorbeeld: *leerlingen kunnen geen les krijgen door door uitvallen kritieke systemen,* en/of: *back-ups met o.a. leerlinggegevens gaan verloren (met alle gevolgen van dien...)*

PO RAAD VO RAAD

Dreiging 3: Identiteitsfraude en manipulatie van data

- Manipulatie van cijfers of toegang tot accounts van docenten
- Door gebrek aan technische maatregelen zoals tweefactorauthenticatie

Voorbeeld: *fraude door een leerling met cijfers*

PO RAAD VO RAAD

Wat kun je met het dreigingsbeeld?

- Vertaling: generiek naar specifiek
- Welke risico’s loop je als schoolbestuur?
- Welke maatregelen kun je nemen?
  - Normenkader
  - Basismaatregelen
- Gesprek aangaan binnen je organisatie

PO RAAD VO RAAD

Aan de slag…

- 2 cases over cyberincidenten, start met verteller: ogen dicht = extra inleving!
- De feiten op een rij
- In groepjes in discussie over de vragen
- Plenaire bespreking
- Onze aanbevelingen en tips

PO RAAD VO RAAD

Case 1: Milan en het dreigbericht (20 min)

Case 1: de feiten

- De school formeerde op zaterdagavond een **crisisteam**.
- De politie deed **forensisch onderzoek**, in samenwerking met de school en de leverancier van het leerlingvolgsysteem.
- De **media** berichtte groots over het incident. Er waren foto's van de arrestatie gemaakt door buurtgenoten van Milan.
- **5 ouders** schreven hun kind in hetzelfde weekend op een andere school in.
- Op zondag bleek het leerling account van Milan te zijn **gehackt**. Milan mocht naar huis.
- Ook al ging het om een hack, de **dreiging** bleef overeind. Op maandag – er stond toevallig een studiedag gepland - is de school doorzocht door de politie.
- De school **communiceerde** continu open met leerlingen, ouders en medewerkers.
- De school regelde **psychische ondersteuning** voor Milan, leerlingen en medewerkers.
- Op dinsdag ging de school open. Maar leerlingen en medewerkers **voelden zich erg onveilig**.
- Ouders eisten beveiliging, tassencontroles en wapenpoortjes. **De school is twee weken lang beveiligd.**
- Na twee weken kwam Milan weer naar school. Hij werd ondanks zijn **onschuld** met argusogen bekeken door medeleerlingen en ouders.
- De school deed **aangifte** van de bedreiging.
- **Er heeft nooit een schietincident plaatsgevonden.**

NB: de naam Milan is gefingeerd. Deze case is gebaseerd op een waargebeurd incident.

Case 1: bespreking (5 min)

Wat kwam er naar voren in jullie groepje?

Wat waren de voornaamste inzichten?

Case 1: aanbevelingen / tips

Crisismanagement / schadebeperking: Stel een cybercrisisplan op.
- zie norm 6.1, 6.2 en 6.3 uit het Normenkader IBP FO
- ...en de hulpmiddelen voor incidentmanagement op Aanpak IBP (Kennisnet)

Preventie: Hanteer een gedegen wachtwoordenbeleid.
- zie de maatregelen in het Normenkader IBP FO
- … en de informatie over wachtwoordbeleid op Aanpak IBP (Kennisnet)

En verder:
- Aangifte doen bij de politie helpt. (Vraag bij het bellen naar een cyberrechercheur!)
- Maak binnen 72 uur van een dergelijk incident melding bij de Autoriteit Persoonsgegevens.

Waarom? Zonder aangifte van een cyberincident kunnen daders nooit worden opgespoord.
Aangiftes en meldingen zorgen voor een hogere bewustwording van risico's.
Daarnaast kunnen andere scholen en instanties ervan leren.

Case 2: Persoonsgegevens op straat (20 min)

Case 2: bespreking (5 min)

Wat kwam er naar voren in jullie groepje?

Wat waren de voornaamste inzichten?

Case 2: aanbevelingen / tips

- **Datalekken** komen het meeste voor bij scholen. Vaak door onhandigheid.
- Op dag 4 werd melding gedaan bij de **Autoriteit Persoonsgegevens**. Dat is te laat, het moet binnen 72 uur.
- **Zorg voor een back-up en herstelplan**

https://aanpakibp.kennisnet.nl/back-up-en-herstelplan/
Norm 13 *IT-operatie*

PO RAAD VO RAAD

Case 2: aanbevelingen / tips

Preventie: Scherp wachtwoordenbeleid aan (gebruik daarvoor het Normenkader IBP FO en de informatie op Aanpak IBP - https://aanpakibp.kennisnet.nl/wachtwoordbeleid/)

Preventie: Stel toegangsbeleid op en koppel deze met het uitdiensttredingsproces

- Handreiking Toegangsbeleid – VNG https://www.informatiebeveiligingsdienst.nl/product/toegangsbeleid/
- Norm 10 *Identity & Access Management*, Norm 4.4 *Verandering of beëindiging van functie*

PO RAAD VO RAAD

Video's cyberincidenten

- Een hack en gijzelsoftware: denk niet dat het jou niet overkomt on Vimeo
- Organisatie gehackt en gegevens op straat? Snel en zorgvuldig handelen! on Vimeo
- Veilig e-mailen: hoe een klein, menselijk foutje tot een datalek kan leiden on Vimeo
- Een dreigmail via een gehackt leerling-account: kalm blijven en snel handelen on Vimeo

Hoe digitaal veilig is jouw organisatie?

Vragen?

- Wat nemen jullie uit deze workshop mee de schoolorganisatie in?
- Vragen?

Contact: digitalisering@povosi.nl