Het herkennen van een Jong Cyberbrein en dan?

Handleiding herkenning voor docenten versie 1

Stichting Cyberbrein.nl

Gemeente Almere

Sneek, september 2024

Een cyberbrein: hoe herken je dat nu?

Een "jong cyberbrein" is gedefinieerd als een jongere met een uitzonderlijk talent en interesse in computers en digitale technologieën. Deze kinderen vallen op door hun vermogen om complexe taken uit te voeren met een computer, wat ver boven het niveau van hun leeftijdsgenoten ligt. Uit de theorie komen kenmerken van jonge cyberbreinen zoals:

1. **Opmerkelijke kennis en interesse in computers en digitale systemen:** Deze kinderen hebben een diepe nieuwsgierigheid naar hoe technologie werkt en het kan maar zo zijn dat ze al programmeren bijvoorbeeld.
2. **Halen graag dingen uit elkaar** om hun werking te begrijpen.
3. **Hyperfocus en probleemoplossend vermogen:** Ze kunnen zich intensief richten op problemen totdat deze zijn opgelost.
4. **Creativiteit:** Ze bedenken vaak out-of-the-box oplossingen voor problemen.
5. **Autodidactisch vermogen:** Ze leren vaak zelfstandig en ontwikkelen hun vaardigheden zonder veel externe hulp.
6. **Goede beheersing van de Engelse taal:** Omdat veel van hun tijd online wordt doorgebracht, spreken en begrijpen ze vaak goed Engels.
7. **Analytische vaardigheden:** Ze zijn goed in het analyseren en begrijpen van complexe systemen en situaties.
8. **Minder offline sociale contacten:** Ze hebben meestal meer online contacten dan offline relaties.

Ethical hackers en ouders vullen hier vaak nog deze kenmerken op aan:

9. **Eerlijk:** ze zeggen wat ze zien ongeacht de context/situatie/gesprekspartner;
10. Door een **sterk gevoel voor rechtvaardigheid** lopen ze niet zomaar mee in de maatschappelijke ordening met regels en systemen. Zeker als regels niet logisch zijn, kan dat leiden tot **dwars** gedrag;
11. **Hulpvaardig:** helpen vaak de juf of meester met allerlei ICT-vragen maar ook anderen in hun sociale context. Ook als daar niet altijd om gevraagd wordt;
12. **Eigen-wijs:** cyberbreinen hebben vaak een “andere” manier van leren is en komen soms op heel creatieve wijze tot oplossingen/antwoorden. Niet altijd volgens het boekje maar wel een goed antwoord.

Deze kenmerken maken het mogelijk om het talent van deze kinderen vroegtijdig te leren herkennen en ze daarna te kunnen begeleiden zodat ze hun

talenten op een positieve manier kunnen ontwikkelen en niet het criminele pad opgaan.

Motivaties om te hacken

Uit onderzoek blijkt dat de belangrijkste positieve motivaties voor jonge cyberbreinen om te gaan hacken zijn:

1. **Nieuwsgierigheid**:
    - Veel jonge hackers worden gedreven door een diepe nieuwsgierigheid naar hoe dingen werken in de digitale wereld. Ze willen de geheimen van technologie ontrafelen en begrijpen hoe systemen en netwerken functioneren.
2. **Uitdaging en Spanning**:
    - De spanning en uitdaging van het hacken trekken veel jongeren aan. Het is een intellectuele puzzel die hen uitdaagt om hun technische vaardigheden en probleemoplossend vermogen te testen en te verbeteren.
3. **Digitale Veiligheid**:
    - Een aantal jonge hackers begint met hacken vanuit een gevoel van verantwoordelijkheid voor digitale veiligheid. Ze willen kwetsbaarheden in systemen ontdekken en deze melden om de veiligheid van deze systemen te verbeteren.
4. **Experimenteren en Leren**:
    - Jonge cyberbreinen vinden het leuk om te experimenteren met technologie. Het proces van proberen, falen en leren is voor hen zeer motiverend. Dit hands-on leren helpt hen om hun vaardigheden verder te ontwikkelen en te verfijnen.

Deze motivaties zijn sterk gekoppeld aan de behoefte van jonge cyberbreinen om te begrijpen, te creëren en bij te dragen aan een veiligere digitale omgeving.

En dan?

Denk je nu? Hee maar dan ken ik wel een mogelijk cyberbrein. Dan zouden we vanuit het project Cyberbreinen in Beeld graag kijken hoe we dit cyberbrein

kunnen begeleiden om zijn talent op een goede manier te leren inzetten en te ontwikkelen. Graag kijken we naar mogelijkheden in Almere dan wel landelijk.

Je kan hiervoor altijd contact opnemen met:

Henk van Ee (Stichting Cyberbrein.nl)

Tel:06-42158182

Henk.van.ee@cyberbrein.nl

Talent gebruiken op school

Hier zijn een aantal tips om jonge cyberbreinen op een positieve manier in te zetten om de school veiliger te houden:

1. **Organiseer een Cybersecurity Club of Werkgroep:** Creëer een speciale club of werkgroep waar jonge cyberbreinen samen kunnen komen om hun kennis en vaardigheden te delen. Binnen deze groep kunnen ze werken aan projecten die de digitale veiligheid van de school verbeteren, zoals het controleren van netwerkbeveiliging of het ontwikkelen van bewustwordingscampagnes voor medeleerlingen.
2. **Stimuleer Ethical Hacking:** Bied lesmodules of workshops aan over ethical hacking. Leg uit wat ethical hacking inhoudt en waarom het belangrijk is. Laat de leerlingen onder begeleiding van een IT-expert of docent met kennis van zaken ethische hackmethoden toepassen op de schoolnetwerken om kwetsbaarheden te identificeren en op te lossen. Dit kan hun technische vaardigheden verbeteren en tegelijkertijd bijdragen aan de veiligheid van de school.
3. **Betrek ze bij Technische Ondersteuning:** Maak jonge cyberbreinen onderdeel van het IT-ondersteuningsteam van de school. Ze kunnen helpen bij het oplossen van technische problemen, het onderhouden van hardware en software, en het monitoren van het netwerk voor verdachte activiteiten. Dit geeft hen praktische ervaring en zorgt ervoor dat ze actief bijdragen aan een veilige schoolomgeving.
4. **Implementeer Cybersecurity Projecten:** Geef deze leerlingen verantwoordelijkheid over specifieke cybersecurity projecten, zoals het ontwikkelen van een veilig wachtwoordbeleid of het opzetten van een veilige opslag voor gevoelige gegevens. Dit kan in de vorm van een schoolproject of een extra-curriculaire activiteit. Zorg ervoor dat ze regelmatig hun bevindingen en verbeteringen presenteren aan de

schoolleiding en hun medeleerlingen, zodat hun werk erkend en gewaardeerd wordt.

Door deze tips te volgen, kunnen docenten niet alleen de digitale veiligheid van de school verbeteren, maar ook de talenten van jonge cyberbreinen op een positieve manier benutten en hen aanmoedigen om hun vaardigheden verder te ontwikkelen in een ethische en constructieve richting.

Talent buiten school

Deze tips kunnen ook buiten school natuurlijk. Laat jonge cyberbreinen meehelpen de digitale veiligheid van organisaties/sportclubs/gemeentes onderzoeken bijvoorbeeld.

In Den Haag zijn hier goede ervaringen mee opgedaan: https://www.hackthehague.com/

Hack the Hague is een jaarlijkse ethische hackwedstrijd georganiseerd door de gemeente Den Haag in samenwerking met cybersecuritypartners. Tijdens dit evenement worden ethische hackers uitgenodigd om kwetsbaarheden in de digitale infrastructuur van de gemeente op te sporen. Het doel is om de cyberweerbaarheid van de stad te vergroten door potentiële beveiligingslekken te identificeren en op te lossen voordat kwaadwillenden hiervan misbruik kunnen maken. Deelnemers kunnen zowel individuele hackers als teams zijn, en er zijn prijzen te winnen voor de beste bevindingen. Door deze wedstrijd stimuleert de gemeente Den Haag de samenwerking tussen overheid en cybersecurity-experts om samen een veiligere digitale omgeving te creëren.

Leren en Doen

Hieronder een aantal mogelijkheden voor jonge cyberbreinen om te leren op diverse platformen.

- **Codecademy:**
  - Omschrijving: Een online leerplatform dat interactieve cursussen biedt in verschillende programmeertalen zoals Python, JavaScript, HTML, CSS en meer.

- Doel: Het toegankelijk maken van coderen en programmeren voor iedereen, van beginners tot gevorderden.

- **VulnHub:**
  - **Omschrijving:** Een platform dat gratis virtuele machines en applicaties biedt voor beveiligingstrainingen en pentesten.
  - **Doel:** Het bieden van een veilige omgeving voor beveiligingsonderzoekers om hun vaardigheden in kwetsbaarheidsanalyse en ethisch hacken te verbeteren.

- **DIVD Academy:**
  - **Omschrijving:** Een onderdeel van het Dutch Institute for Vulnerability Disclosure (DIVD), gericht op het trainen van mensen in cybersecurity en kwetsbaarheidsdetectie.
  - **Doel:** Het verhogen van het kennisniveau en de vaardigheden in cybersecurity binnen Nederland door middel van trainingen en workshops.

- **Challenge the Cyber:**
  - **Omschrijving:** Een competitie gericht op jongeren om hun cybervaardigheden te testen en te verbeteren door middel van uitdagende opdrachten en scenario's.
  - **Doel:** Het identificeren en stimuleren van jong cybertalent en het vergroten van hun interesse en vaardigheden in cybersecurity.

- **Stichting Cyberbrein.nl:**
  - **Omschrijving:** Een organisatie die zich richt op het identificeren en begeleiden van jong cybertalent om hen te helpen hun vaardigheden op een positieve manier te ontwikkelen.
  - **Doel:** Het voorkomen dat jong talent afglijdt naar cybercriminaliteit door hen te ondersteunen en te begeleiden naar ethische en professionele toepassingen van hun vaardigheden.

HackShield:
  - **Omschrijving:** HackShield is een educatief spel dat kinderen tussen de 8 en 12 jaar leert over cybersecurity en online veiligheid door middel van gamification. Ook in varianten die gericht zijn op Ethical Hacking;
  - **Doel:** Het bewustmaken van kinderen over de gevaren van het internet en hen leren hoe ze zichzelf en anderen kunnen beschermen tegen cyberdreigingen. Het spel combineert avontuur en educatie om

de interesse van jonge kinderen te wekken en hen waardevolle cybersecurity vaardigheden bij te brengen.

FreeCodeCamp:

- **Omschrijving:** FreeCodeCamp is een non-profit online platform dat gratis cursussen en certificeringen biedt in webontwikkeling en programmeren. De cursussen omvatten onderwerpen zoals HTML, CSS, JavaScript, Python, en meer.
- **Doel:** Het toegankelijk maken van programmeer- en webontwikkelingsonderwijs voor iedereen, ongeacht hun achtergrond of financiële situatie. Het platform biedt ook hands-on projecten en een gemeenschap van lerenden om samen te werken en elkaar te ondersteunen.