mbo digitaal

Red teaming

SAMENWERKEN AAN
CYBERVEILIGHEID
IN HET MBO

11 december 2025

Mick Deben & Ry Boxem

mbo digitaal

Agenda

Introductie

Methodiek

Uitdagingen

Resultaten

Toekomst Red teaming?

mbo digitaal

Introductie

- **Doel van deze workshop:**
  - Delen van ervaringen met Red Teaming bij mbo’s
  - Blik werpen op toekomst van Red Teaming voor mbo’s

- **Wat is Red Teaming:**

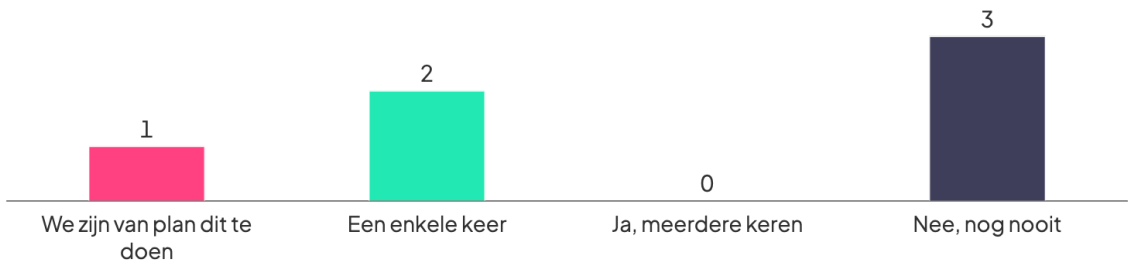
  een realistische aanvalssimulatie waarbij ethische hackers optreden als echte tegenstanders om de weerbaarheid van een organisatie te testen.

- **Belang van Red Teaming:**

  observeren hoe een organisatie presteert onder realistische aanvalsscenario’s, iets wat traditionele pentests niet (volledig) zichtbaar maken. Het helpt onderwijsinstellingen gericht te investeren in verbeteringen die daadwerkelijk effect hebben op hun digitale weerbaarheid.

Poll

Hebben jullie als onderwijsinstelling ooit een Red Team-test laten uitvoeren?



mbo digitaal

Methodiek - VCTH

Voor de Red Team-trajecten bij mbo-instellingen hebben we eerst een **voortraject** doorlopen, ’van check tot hack’. Dit voortraject was bedoeld om de basisrisico’s in kaart te brengen en eventuele bekende zwakheden te verhelpen, zodat het Red Team zich volledig kon richten op de meer geavanceerde aanvalspaden.

Het voortraject bestond uit meerdere onderdelen, waarvan de volgende directe impact hadden op Red Teaming

- **Kwetsbaarhedenscan:** een technische scan om bekende kwetsbaarheden snel zichtbaar te maken.
- **OSINT-rapport:** onderzoek naar publiek beschikbare informatie die door aanvallers gebruikt kan worden.
- **Netwerkpentest:** een gerichte test om eenvoudig misbruikbare zwakheden te identificeren en weg te nemen — het “gras maaien” vóór de voeten van het Red Team.

Door deze voorbereidende stappen werd het Red Team in staat gesteld om realistischer en effectiever te testen, met focus op weerbaarheid in plaats van laaghangend fruit.

mbo digitaal

Methodiek - VCTH

Netwerkpentest: een gerichte test om eenvoudig misbruikbare zwakheden te identificeren en weg te nemen — het “gras maaien” vóór de voeten van het Red Team.

mbo digitaal

Methodiek – ART SURF

Red Teaming met methodiek

- Gestandaardiseerde structuur met vaste fases en scenario’s
- Duidelijke doelstellingen en uniformere scope
- Focus op realistische dreigingsscenario’s in de sector
- Aanleveren van een dreigingsrapport en threat intelligence
- Detectie, weerbaarheid en respons in lijn met dreigingsscenario’s

professionaliseringsslag van red teaming!

mbo digitaal

Inzoomen – ART SURF

mbo digitaal

Inzoomen – ART SURF

mbo digitaal

Inzoomen – ART SURF

mbo digitaal

Inzoomen – ART SURF

mbo digitaal

Inzoomen – ART SURF

mbo digitaal

Inzoomen – ART SURF

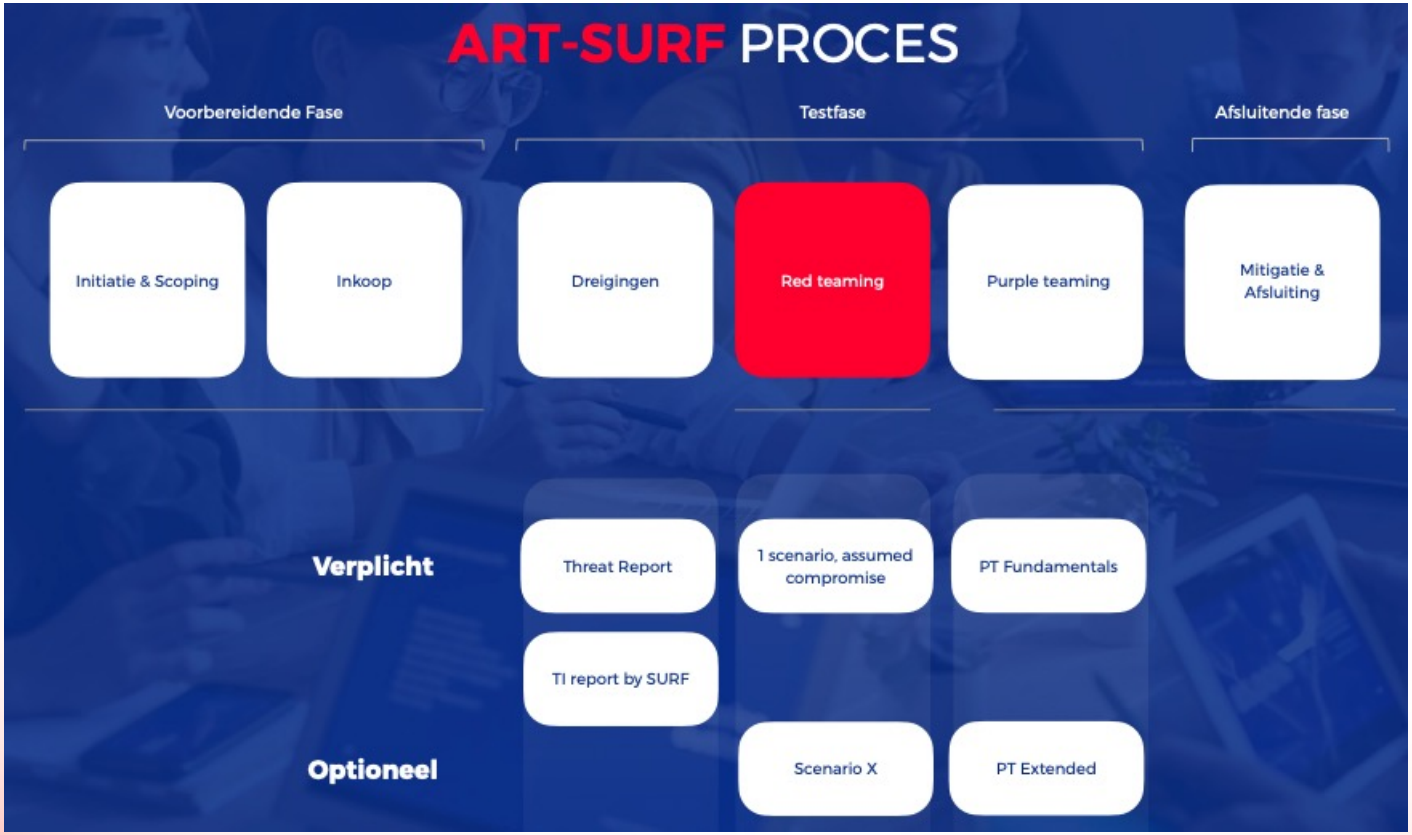
mbo digitaal

Inzoomen – ART SURF

- Geleerde lessen uit andere sectoren:
  - ART/TIBER is een waardevolle toevoeging bovenop bestaande testen en compliance
  - Organisaties leren al veel van de Scoping en Threat Intelligence fasen
  - Cyber Resillience is verbeterd, waardoor het voor red teams (en dreigingsactoren) moeilijker wordt om te slagen
  - Doordat je samen de testen ondergaat ontstaat er een community waarin lessen kunnen worden gedeeld

mbo digitaal

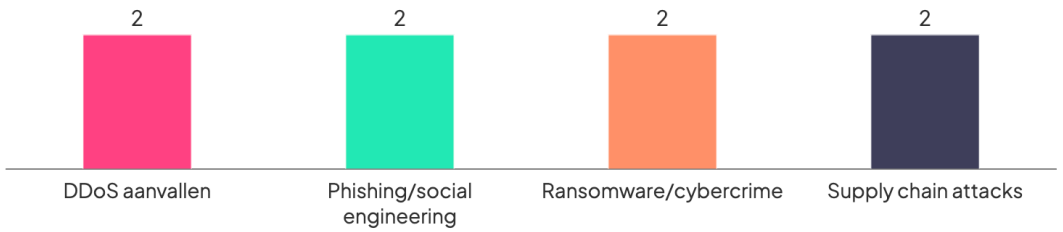
Inzoomen – ART SURF



mbo digitaal

Poll

Welke dreiging zien jullie als het grootste voor mbo-instellingen?



mbo digitaal

Inzoomen – ART SURF

Uitkomst TI:

De meest recente Quarterly Cyber Threat Report van GEANT voor Europese onderwijs en onderzoeksinstellingen (gemaakt met medewerking van SURF) geeft een dreigingsbeeld voor het onderwijs. Er zijn 2 primaire dreigingen die in dit rapport naar voren komen: Spionage (vergaren van intelectueel eigendom en/of inlichtingen) door statelijke actoren en Ransomware/Cybercrime voornamelijk door oppertunistische actoren. MBO's ontwikkelen geen intelectueel eigendom wat van waarde is voor statelijke actoren.

Voor het dreigingsbeeld blijft dan over Ransomeware/Cybercrime. Dit is compleet in lijn met ervaringen van (bijna)incidenten bij mbo's in de afgelopen jaren.

De voornaamste threat actors voor Ransomware volgens GEANT zijn:
- Fog
- Interlock
- SafePay
- Qilin

Echter gezien het oppertunisme is het waarschijnlijk dat andere threat actors met vergelijkbare technieken en doelstellingen onderdeel zijn van het dreigingslandschap voor [..].

mbo digitaal

Poll

Hoe snel gaan aanvallen anno 2025

mbo digitaal

Inzoomen – ART SURF

Conclusie Red Team:

[...] heeft een gesimuleerde Red Team uitgevoerd op het netwerk van [...] en kroop in de rol van een ransomware aanvaller. Deze Red Team test heeft laten zien dat [...] grotendeels is voorbereid op cyberdreigingen van een dergelijke actor.

Met slechts 12 bevindingen en geen volledig compromittering in drie weken tijd, is duidelijk dat de organisatie al een sterke basis heeft om de systemen te beveiligen. Daarnaast is het ook gelukt om de aanvallers te detecteren en was het daarmee gelukt om de aanvallers de toegang tot het netwerk te ontzeggen.

mbo digitaal

Vergelijken leveranciers

Leverancier A

- ’In’ fase kreeg veel aandacht
- Bij assume breach snel rechten willen verhogen
- Taal en cultuur barriere

Leverancier B

- Direct assume breach
- Bredere scope, minder focus op AD, meer op kwetsbare applicaties en beschikbare informatie op het netwerk.

mbo digitaal

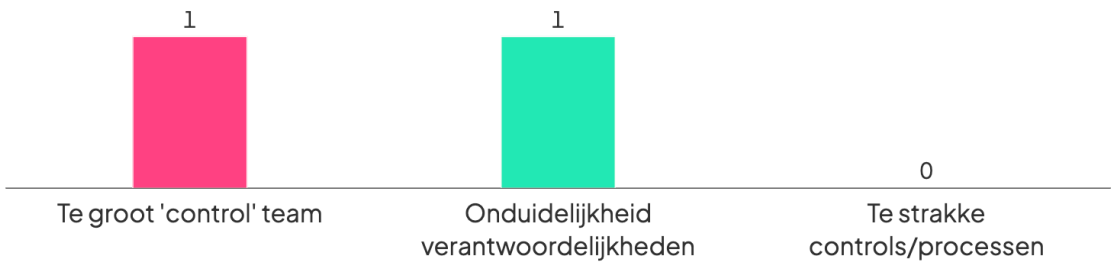
Uitdagingen Red Teaming

- Voorbereidende werkzaamheden (voortraject voor een methodisch goede test) kosten veel tijd.
  - Maar! Veel stappen zijn herbruikbaar en/of te automatiseren.
- Leg-ups / Assume breach, blijkt lastig te realiseren wanneer het control team klein gehouden wordt.
- Leveranciers van de te testen instelling kunnen voor veel vertraging en ruis zorgen.

mbo digitaal

Poll

Welke problemen voorzie je bij het maken van een leg-up voor een redteam actie?



mbo digitaal

Resultaten

Onderwerp	Aanbeveling
Beveiliging van Werkstations en Servers	Hardening op de Domain Controllers (LDAP signing verplichten)
	Clear-text credentials in network shares, Sharepoint, etc. opsporen en vermijden
Netwerkbeveiliging	Filteren netwerkverkeer van DC's naar andere subnets
Active Directory-beveiliging	Verder afstemmen van het wachtwoordbeleid op het type account (gebruiker, administrator, service)
	Kleinere hardening zoals Protected Users, aanmaken van DNS records door users limiteren

mbo digitaal

Resultaten

- Geen MFA op remote werkplek
- Beperkte netwerksegmentatie
- SMB-netwerkmappen
  - Gevonden secrets/keys op netwerkmappen
  - Beheerapplicaties beschikbaar op netwerkmappen
  - Bevindingen uit eerdere pentest beschikbaar
- Onbeperkt gebruik powershell op werkplek
  - LOLBINS beschikbaar op werkplek
  - SSH naar buiten mogelijk

mbo digitaal

Resultaten

Tijdens de trajecten waarbij we een red team inzetten dat ook de volledige ‘IN’-fase testte werd een duidelijke conclusie getrokken. De leverancier constateerde dat mbo-instellingen in deze fase over het algemeen zeer goed beveiligd zijn. Veel phishing werd goed afgevangen door de tooling die wijdverspreid is in de sector (Microsoft).

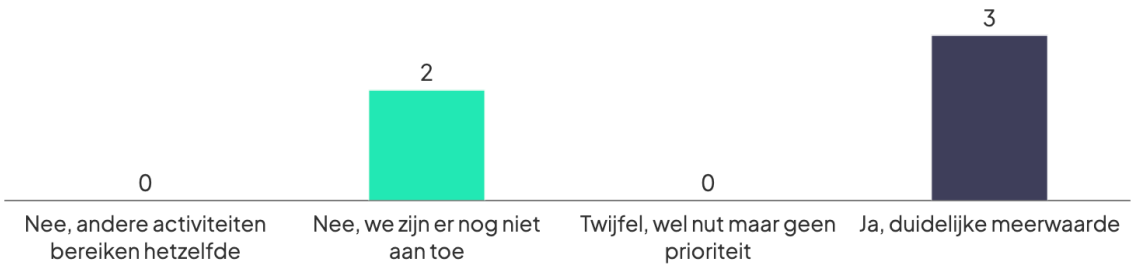
Deze bevinding roept de vraag op hoe waardevol het is om de volledige ‘IN’-fase standaard mee te testen tijdens een red team-assessment, zeker gezien de intensiteit, complexiteit en kosten. Als de kans op succesvolle initial access laag is, kan de toegevoegde waarde van deze fase beperkt zijn in verhouding tot de benodigde investering van instellingen.

Daarnaast gaf de leverancier nog een bredere reflectie: voor organisaties die hun omgeving grotendeels laten beheren door externe leveranciers, aangevuld met een extern SOC, is een traditioneel red team mogelijk niet altijd de meest passende aanpak. In zulke situaties ligt een groot deel van de detectie, monitoring en respons buiten de directe invloedssfeer van de instelling.

mbo digitaal

Poll

Zie je op dit moment voor jouw instellingen meerwaarde in een red team?



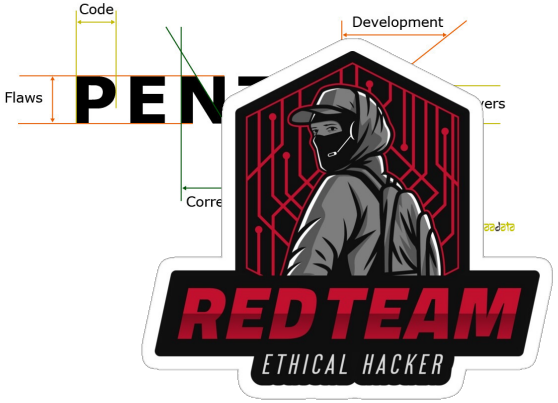
mbo digitaal

Toekomst Red teaming mbo’s

Hackers (1995)

Pool van hackers

Bug bounty



Pentesten + red teaming (huidig wijze)

mbo digitaal

Red teaming

Voor vragen:
m.deben@mbodigitaal.nl
r.boxem@mbodigitaal.nl

MBO Digitaal is een platform van de MBO Raad voor samenwerking aan digitalisering in het mbo. MBO Digitaal werkt samen met alle mbo-instellingen en heeft sterke banden met MBO Voorzieningen, Kennisnet en SURF.