AFGEHACKT

Hoe houden we onze evenementen digitaal veilig?

RBPO Noord-Nederland
Werkgroep cyberveiligheid

Scherp

NHL STENDEN hogeschool

AFGEHACKT:

Hoe houden we onze evenementen digitaal veilig?

Welke digitale dreigingen zijn er voor evenementen? Wat kunnen we daaraan doen? En wie zijn daarvoor verantwoordelijk?
Over die vragen ontfermde een brede groep experts zich recent bij de kennisdeelsessie Afgehackt, georganiseerd door Scherp in Veiligheid, NHL Stenden Hogeschool/Thorbecke Academie en de werkgroep Cyberveiligheid van RBPO Noord-Nederland.
De deskundigen kwamen vanuit de evenementenbranche, het onderwijs, de overheid en de cybersecuritybranche. Een ding werd duidelijk: er is nog heel wat te doen.

Betrokkenen:

RBPO Noord-Nederland
Werkgroep cyberveiligheid

POLITIE

CCV centrum voor criminaliteitspreventie en veiligheid

Scherp

Gemeente Súdwest-Fryslân

CROWDCOWS

FOXFLOW

NHL STENDEN hogeschool

Drachten Smallingerland

Vinke Vision

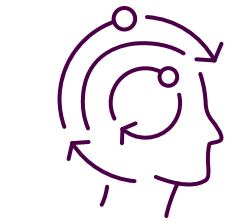
DFR IT Infra & Security

RIEC Noord-Nederland

Gemeente Groningen

PIETER SPOELSTRA PRODUCTIES

Stichting Cyberbrein.nl



Afgehackt is een woordspeling op afgehekt;

Een term uit de evenementenveiligheid, waarmee wordt gerefereerd aan een door hekken afgebakend evenement.

In de paarse kolommen schetsen wij een aantal denkbeeldige scenario's.

Grafisch ontwerp: Beeldende Zaken

RBPO Noord-Nederland
Werkgroep cyberveiligheid

Scherp

NHL STENDEN hogeschool

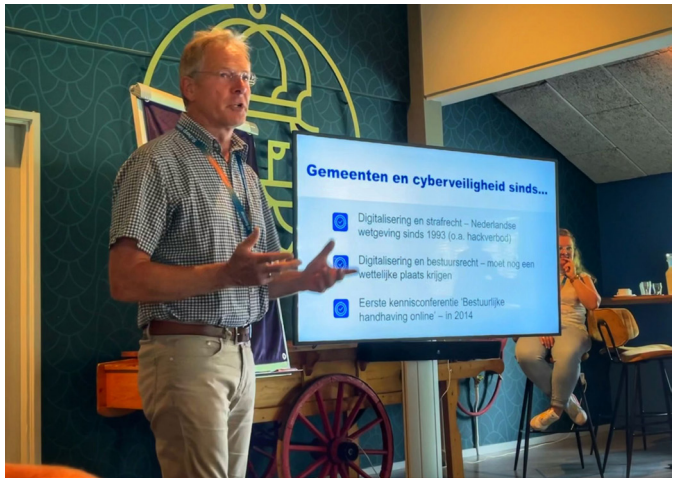
Presentatie Wouter Stol: zorgen om een digitaal Haaksbergen

De sessie in Heerenveen heeft zijn wortels in een essay van lectoren Wouter Stol en Willem Bantema van NHL Stenden Hogeschool Leeuwarden (Bantema & Stol, 2020)*. In dat essay waarschuwden ze voor een Digitaal Haaksbergen, waarbij een cyberincident fysieke gevolgen heeft op een mensenmassa. Ook beschreven ze de rol die gemeenten mogelijk hebben om dat tegen te gaan.

Stol vertelde bij de sessie hier meer over. Daarbij legde hij de deelnemers een vijftal vragen voor over cyberveilige evenementen:

1. Wat zijn de digitale risico's voor de veiligheid van evenementen?
2. Wat valt effectief te doen aan de risico's?
3. Wie gaan aan de slag met de risico's?
4. Heeft die partij bevoegdheden/mogelijkheden?
5. Hoe organiseert die partij wat ze moet doen?

Op deze vragen zijn met aanwezige experts verder verkend bij de sessie Afgehackt.



Wat zijn de risico's?

Denkbeeldige scenario's over dreigingen zijn er genoeg, zo bleek tijdens de sessie. Van gehackte toegangspoortjes tot gesaboteerde led-schermen die het publiek de verkeerde kant opsturen; volgens een deelnemer zijn er wel 100.000 scenario's te bedenken. Doden en gewonden zijn daarbij niet uitgesloten, en een deelnemer noemde het scenario Loveparade 2.0. Daarbij refereerde hij aan een festival in Duitsland, waarbij meerdere slachtoffers vielen door verdrukking (NOS, 2015)*. Zoiets kan ook gebeuren als een festival digitaal wordt gesaboteerd.

Maar hoe groot is het daadwerkelijke risico op zo'n scenario? Volgens een aanwezige cyberexpert is "alles met een ip-adres te hacken". Aangezien evenementen steeds digitaler worden lijken de risico's dus op zijn minst aanwezig. Een adviseur veiligheid van een gemeente benadrukte ook dat de risico's voor alle evenementen geldt, van grote festivals tot kleinschalige buurtfeesten. Denk bijvoorbeeld aan een slecht beveiligde website van een buurtfeest, met daarop persoonsgegevens voor aanmeldingen en van vrijwilligers.

* Stol, W.Ph. & W. Bantema (2020) Stadsbestuur en digitale veiligheid. Een analyse van beleidsplannen. In M. Malsch en J. W. Sap (red.) Orde en verwarring in de stad. Den Haag: Boom Criminologie, pp. 363-385.
* NOS. (2015, 24 juli). 2010: *Toen de Love Parade een dodendans werd. NOS.* **(meer informatie)**

RBPO Noord-Nederland
Werkgroep cyberveiligheid

Scherp

NHL STENDEN hogeschool

Scenario's: Winterspelen en voetbalstadion gehackt

In Nederland zijn nog weinig voorbeelden bekend van evenementen waarbij een cyberincident een ontwrichtend fysiek effect had. Er zijn wel Nederlandse voorbeelden bekend van datalekken bij evenementen. In het rapport Digitale Veiligheid Evenementen van de Rijksuniversiteit Groningen uit 2018 vertelde een respondent ook dat zijn ticketsysteem weleens is gehackt, wat tot lange rijen leidde (Asllani et al., 2018)*.

In het buitenland zijn meerdere casussen van gehackte evenementen bekend:

- de Winterspelen in Zuid-Korea in 2018 (Greenberg & Excerpt, 2019)*. Bij deze hack werd onder meer de website offline gehaald, waardoor tickets niet geprint konden worden en veel bezoekers de openingsceremonie misten.
- Zuidoost-Aziatische Spelen in 2015 (Hussain, 2016)*. Hierbij is onder meer de controle over beveiligingscamera's overgenomen door hackers.
- Britse voetbalclub (National Cyber Security Centre, 2020)*. Hierbij zijn toegangspoortjes in het stadion gesaboteerd.

Over de omvang van de dreiging vallen dus nog weinig harde conclusies te trekken, al is het realistisch om te stellen dat digitale risico's de veiligheid van een evenement kunnen aantasten. Onder de deelnemers was ook consensus dat meer onderzoek nodig is om de risico's te bepalen. NHL Stenden Hogeschool is in september 2023 gestart met een brede verkenning voor de VNG naar digitale veiligheid bij bedrijven en mogelijkheden van vergunningverlening. Daarin is digitale veiligheid van evenementen een onderdeel en er zijn meer plannen voor onderzoek. Een cyberexpert pleitte ervoor om als proef ethische hackers aan het werk te zetten bij evenementen, om zo kwetsbaarheden te vinden.

DENKBEELDIG SCENARIO:

Data bezoekers op straat

De jaarlijkse erotiekbeurs Stout staat voor de deur. De organisator heeft duizenden kaartjes verkocht. Maar een paar dagen voor de start komt een vervelend bericht binnen: een hacker heeft bestanden gestolen.
De hacker claimt dat er ook persoons- en betaalgegevens bij zitten van mensen die een kaartje hebben gekocht voor de beurs, en hij dreigt die te publiceren. Tenzij de organisatie twee ton betaalt. Om te laten zien dat het menens is, stuurt de hacker een lijst met dertig namen van bezoekers naar de organisatie. Hij heeft de gegevens dus echt.

* Asllani, E., Van den Berg, A., Hofman, E., & Xue, L. (2018, July 19). *Rapport Digitale Veiligheid Evenementen*. (meer informatie)
* Hussain, A. (2016, October 5). *Engineer gets 8 months' jail for hacking into police CCTV cameras at SEA Games 2015*. The Straits Times. Retrieved July 25, 2023 (meer informatie)
* Greenberg, A., & Excerpt. (2019, October 17). *Inside Olympic Destroyer, the most deceptive hack in history. WIRED.* (meer informatie)
* National Cyber Security Centre. (2020, July 23). *The cyber threat to sports organisations*. Retrieved July 25, 2023 (meer informatie)

RBPO Noord-Nederland
Werkgroep cyberveiligheid

Scherp

NHL STENDEN hogeschool

Welke maatregelen kunnen we nemen?

Naast het onderzoek van NHL en de hackproeven zijn meer oplossingsrichtingen geopperd bij de sessie:

Digitale veiligheid als voorwaarde voor een vergunning
Dit idee van Stol en Bantema werd omarmd door de meerderheid van de deelnemers.
Oftewel; wil een organisatie een vergunning voor een evenement? Dan toont de organisator eerst aan de gemeente aan dat de digitale veiligheid op orde is.

Het opstellen van een normenkader voor cybersecurity bij evenementen
Op basis van dit kader kan een organisatie de digitale veiligheid versterken en laten controleren. Op termijn kan daar een keurmerk aan gekoppeld worden. Op kortere termijn moet vooral worden gewerkt aan het bewustzijn van de risico's onder de belanghebbenden.
"Het zou al een mooie stap zijn als dit risico wordt meegenomen in de risicoanalyse", aldus een deelnemer vanuit de evenementen branche.

Digitale veiligheid prioriteit maken bij organisatoren
Hiervan is momenteel nog geen sprake, volgens het rapport Digitale Veiligheid Evenementen, waaraan we op de vorige pagina refereren. Bij de sessie werd dit bevestigd en ook deels verklaard: de regeldruk groeit. Organisatoren van evenementen krijgen jaarlijks te maken met meer regels en voorschriften waar ze aan moeten voldoen. De zorg werd geuit dat het opleggen van cybervoorschriften een negatieve impact heeft op de bereidwilligheid voor het organiseren van evenementen.

En er zijn meer manieren te bedenken om cyberveiligheid bij evenementen te verbeteren. Zo kan het thema een plek krijgen in het Handboek Evenementenveiligheid en kunnen veiligheidsregio's het onderwerp meenemen in hun advies aan organisatoren. Ook kan een database voor cyberincidenten bij evenementen helpen, om meer inzicht te krijgen in het risico en om van eerdere incidenten te leren.

DENKBEELDIG SCENARIO:

Gehackt ticketsysteem

Eindelijk: na jaren van corona kan het SUPERHARD-festival weer doorgaan. Er zijn tienduizenden mensen afgekomen op het festival, waar voornamelijk hardcore, hardstyle en andere elektronische muziek wordt gedraaid. Tienduizenden mensen hebben een kaartje gekocht. Maar aan het begin van de avond begint het ticketapparaat te haperen. Geen enkel ticket lijkt te werken, en de mensenmassa voor de ingangen groeit. Er ontstaan opstootjes en mensen raken in de verdrukking.

RBPO Noord-Nederland
Werkgroep cyberveiligheid

Scherp

NHL STENDEN
hogeschool

DENKBEELDIG SCENARIO:

Gehacke kermis

Het is druk op de jaarlijkse kermis in Ottemeer. De kermis is een van de drukst bezochte evenementen in de streek, en is zelfs een van de grootste kermissen van Nederland. De populariteit komt deels door de spectaculaire attracties die op de kermis staan. Een daarvan is het nieuwe spookhuis. Het is niet een typisch spookhuis, maar een 'state of the art digital driven interactive haunted house'. Een soort moderne Droomvlucht. Bezoekers kunnen hun mobiele telefoon koppelen aan de attractie, en zo dingen laten gebeuren. Zo zitten de bezoekers in een soort achtbaankarretje op rails dat ze via hun telefoon kunnen besturen. Ook kunnen ze voorwerpen in het spookhuis als schermen en poppen laten bewegen. Het is een populaire attractie, en op zaterdagavond zitten alle karretjes vol. Buiten staan lange rijen met mensen. Zij worden plotseling opgeschrikt door harde knallen en gegil. Hoewel ze in eerste instantie denken dat dit bij de attractie hoort, komen ze er al snel achter dat er meer aan de hand is; de attractie is gehackt. Een crimineel heeft de besturing van het spookhuis overgenomen. De karretjes gaan plotseling op grote snelheid rijden. Sommige botsen op hoge snelheid tegen elkaar, anderen vallen van de rails. Een blijft juist stilstaan en veroorzaakt een kettingbotsing. Het aantal gewonden loopt in de tientallen.

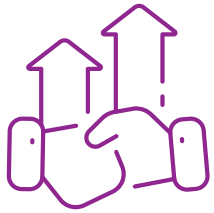
Wie zijn de eigenaren en betrokkenen van dit onderwerp?

Genoeg te doen dus. Maar wie is er aan zet? Volgens de deelnemers zijn de gemeente en evenementenorganisatoren evidente partijen. Zo is de burgemeester formeel verantwoordelijk voor openbare orde in zijn of haar gebied. Maar ook kennisinstellingen, cybersecuritybedrijven, producenten en leveranciers van hard- en software bij evenementen, politie en veiligheidsregio's zijn in meer of mindere mate verantwoordelijk. Meerdere deelnemers brachten ook naar voren dat er nog een 'blinde vlek' is als het gaat om wie verantwoordelijk en/of bevoegd is.

Alle onzekerheden en mogelijke dreigingen ten spijt, het enthousiasme overheerste bij de sessie. Er was een gezamenlijk gevoel van: schouders eronder. Er is veel werk te verrichten om onze evenementen cyberveilig te houden, en er is ook veel mogelijk.

Dus, om Stol nog een keer te citeren:

'nu aan de slag'



Waarom doen we dit?

Scherp in Veiligheid: *Scherp in Veiligheid is een adviesbureau in openbare orde en veiligheid en crisisbeheersing. Wij vinden het belangrijk om bij te dragen aan een veilige maatschappij, onder meer door het kennisniveau te vergroten. Wij zien de digitale risico's voor evenementen en willen ons steentje bijdragen aan het bewustzijn hiervan, en de oplossingen.*
Op termijn kunnen we hiermee onze dienstverlening richting opdrachtgevers uitbreiden.

NHL Stenden Hogeschool: *Binnen de lectoraten van de onderzoeksgroep Cybersafety van de Thorbecke Academie wordt innovatief praktijkgericht onderzoek uitgevoerd. Digitale veiligheid van evenementen past goed bij ons onderzoek en onderwijs naar digitale weerbaarheid en ook uitstekend bij het pionierende en vernieuwende karakter van ons onderzoek dat onder andere gericht is op het bijdragen aan een openbaar bestuur (governance) dat effectief kan anticiperen op een steeds verder digitaliserende samenleving. Bijdragen aan nieuwe kennis en het breed uitdragen van kennis is onze kracht.*

Werkgroep cyberveiligheid van RBPO Noord-Nederland:
In het regionaal veiligheidsplan van Noord-Nederland is het bevorderen van cyberveiligheid geprioriteerd. Om invulling te geven aan die ambitie is een ambtelijke werkgroep cyberveiligheid in het leven geroepen. Daarin zijn onder onder andere gemeenten, politie, het Openbaar Ministerie en het RIEC Noord-Nederland vertegenwoordigd. De werkgroep houdt zich bezig met het bestuurlijk en ambtelijk agenderen en het aanjagen van beweging op het thema. We zetten ons gezamenlijke netwerk in om zicht te krijgen op actuele cyberveiligheidsproblemen en om bij te dragen aan de aanpak daarvan. De digitale veiligheid van evenementen is een van de thema's waarin de werkgroep zich vastbijt.


AFGEHACKT
OPBRENGST KENNISDEELSESSIE 11 JULI 2023
RBPO Noord-Nederland
Werkgroep cyberveiligheid
Scherp
NHL STENDEN hogeschool
VERSCHILLENDE PERSPECTIEVEN
GEVOLGEN
CRISIS
ORDEVERSTORING
SCHADE
VAN IEDEREEN VAN NIEMAND
TECHNIEK
VEILIGE WIFI, PIN, TICKET
WIE?
HOUDING SPEELT BIJ ONS NIET
CYBERVEILIGE EVENEMENTEN (MENTIMETER)
VERGUNNING NOG GEEN 'ONLINE' AFWEGING
KIJKEN MET HALVE BRIL
SCENARIO'S ONBEKEND ZIJN VEEL!
RISICO'S
GEEN BIER
FLIPPER OPENT ALLE KASTJES
ALLES MET EEN IP IS TE HACKEN
PERSOONS-GEGEVENS
ONLINE TRIGGER
DIRECT IMPACT
PANIEK
GEWONDEN
ONLINE AANJAGEN
VERGELIJKBAAR MET HAAKSBERGEN
LOVEPARADE
TERUGKIJKEN NET BEGONNEN
1993
2014
NU
HACKVERBOD
IE CONFERENTIE
TAKEN GEMEENTE?
VERGUNNING
GOED? VEILIG? OOK ONLINE?
BGM=HOOFDVERANTWOORDELIJK
CYBER-ADVIES?
IK BEN HOOFD VERANTWOORDELIJK
BEVOEGD GEZAG?
BEZOEKER
BGM
KENNIS-INSTELLING
ORGANISATOR
ONDER-AANNEMER
HOG VOORKOMEN?
WIE BEVOEGD?
TOCH GEBEURD, EN NU?
AU!
PRESENTATIE WOUTER STOL
KETEN
BENOEM VERANTWOORDELIJKHEID
EIGENAREN
BEWUSTZIJN VERGROTEN DOOR KENNIS DELEN
ADVIES-PARTIJEN
NORMEN OPSTELLEN
ISO
SUBSIDIE
FORSE PARAGRAAF IN VEILIGHEIDSPLAN
CYBER KEURMERK
MAATREGELEN
ORGANISEER PROEFTUIN NODIG HACKERS UIT
ONDERZOEK TOEPASBAAR HAKEN NORMEN
BESTUURLIJK AGENDEREN (VNG)
EN NU?
KENNISDOCUMENT 'SPREAD THE WORD'
BETROKKENEN
EXPERTS CYBERVEILIG-HEID
ONDERWIJS
KENNIS- EN ADVIESBEDRIJVEN
EVENT ORGANISATOREN
GEMEENTEN BURGEMEESTER
POLITIE
Tea betekent