CYBERSPRINT
BREAKTHROUGH SECURITY

The Hague
VREDE EN RECHT

E-GUIDE

ZÓ HACK JE EEN STAD / LAND / ORGANISATIE / BEDRIJF / ETC

Hoe gemeente Den Haag haar organisatie klaarstoomt om samen met hackers haar digitale weerbaarheid te verhogen

MAY CONTAIN CYBER

INHOUDSOPGAVE

VOORWOORD

Als (belangrijk) onderdeel van haar beleid ter bevordering van digitale weerbaarheid, organiseert gemeente Den Haag sinds 2017 samen met cybersecuritybedrijf Cybersprint jaarlijks een hack-evenement: Hâck The Hague. Een open en transparant evenement dat wordt gehouden in het Atrium van het gemeentehuis (of online zoals in 2021), waarbij hackers op een gecontroleerde manier worden uitgedaagd om de systemen van de gemeente en die van haar leveranciers te testen op hun digitale veiligheid.

Het succes van dit evenement heeft ertoe geleid dat zowel de gemeente als Cybersprint steeds vaker vragen krijgen van andere gemeenten én het bedrijfsleven over hoe je zoiets organiseert. Hierdoor ontstond het idee om de opgedane ervaringen vast te leggen in een document om deze met een zo groot mogelijke groep van Chief Information Security Officers, ICT- en securitymanagers en beleidsmakers te delen. Niet alleen zodat zij zelf een hack-evenement kunnen organiseren, maar ook om te laten zien wat er nodig is om de kwetsbaarheden in websites en systemen te prioriteren, op te volgen en op te lossen.

In deze e-guide beschrijven we op hoofdlijnen wat er nodig is om uw organisatie voor te bereiden op het continu verbeteren van digitale veiligheid en hoe u hackers hierbij kunt betrekken. U leest het goed: ‘hoe u hackers in kunt zetten om uw digitale weerbaarheid te verhogen’. De term ‘hacker’ heeft voor velen een negatieve connotatie, niet onbegrijpelijk gezien alle berichtgeving rond digitale fraude en inbraken. Daarom is het belangrijk om duidelijk onderscheid te maken tussen eerlijke (ethische) hackers en hackers met criminele intenties (black hat hackers). Ethische hackers zijn maatschappelijk betrokken personen die met hun kennis, inzicht en ervaring een onmisbare schakel vormen in de keten die betrokken is bij het steeds beter beschermen van systemen en informatie. Wanneer we in deze e-guide de term ‘hackers’ gebruiken, dan gaat het over ethische hackers.

Gezien het feit dat digitale veiligheid raakt aan vele onderwerpen, is het onmogelijk om in dit document volledig te zijn. Zo is het belangrijk om vooraf te toetsen of een hacker-evenement past in de lokale wet- en regelgeving waaraan uw organisatie onderhevig is. Onderwerpen waar u in uw voorbereiding ook aandacht aan wilt besteden, maar die niet verder aan bod komen in deze e-guide zijn onder andere:

- Hoe om te gaan met interne politiek, besluitvorming en het verkrijgen van mandaat (deze e-guide kunt u goed gebruiken om gesprekken te starten!).
- Het vaststellen van de volwassenheid en risicobereidheid van de organisatie op het gebied van digitale veiligheid.
- Bepalen wat er nodig is om deze doelstellingen te realiseren en te meten. Denk hierbij aan financiële middelen, capaciteit, kennis, eigen mensen/inhuur etc. Zoek daarbij vooral de samenwerking met bestaande security- en ketenpartners en sector- en branchegenoten.

Heeft u alle voorbereidingen doorlopen, dan kunt u een weloverwogen keuze maken of een hack-evenement iets is voor uw organisatie en op welke manier dit bijdraagt aan het verbeteren van de digitale veiligheid. Vergeleken met het voorwerk dat nodig is om digitale veiligheid integraal onderdeel te maken van uw organisatie, is het opzetten van een hack-evenement relatief eenvoudig. Maar ook dit vraagt om een strakke organisatie en coördinatie. Want pakt het onverhoopt niet goed uit, dan kan een hack-evenement snel uitmonden in negatieve publiciteit bij zowel de hackers als het publiek en in extreme gevallen zelfs datalekken waar niemand op zit te wachten. Komt u tot de conclusie dat een hack-evenement inderdaad een goede aanvulling is op het totale pakket van inspanningen en maatregelen op dit gebied, dan kunt u gebruikmaken van het in deze e-guide uitgewerkte draaiboek voor de organisatie van een hack-wedstrijd.

Het is onmogelijk om alle personen te benoemen die hebben bijgedragen aan de succesvolle edities van Hâck The Hague en daarmee indirect aan deze e-guide. Daarom, zonder iemand daarbij te kort te willen doen, een speciaal dankwoord aan Peter van Eijk voor het delen van zijn kennis en ervaring als Information Security Manager bij gemeente Den Haag en aan hen die een directe inhoudelijke bijdrage hebben geleverd aan de totstandkoming van deze e-guide (in alfabetische volgorde van voornaam):

Chantal Stekelenburg (Head of Operations - Zerocopter), Chris van ’t Hof (Presentator, Onderzoeker, Schrijver en Organisator in informatietechnologie), Daan Rijnders (Lead Cyber Secure - Gemeente Den Haag), Edwin van Andel (CEO

- Zerocopter), Frank Jan Uittenbogaart (Directeur/Manager Product Development - DG Groep), Jonathan Bouman (Huisarts en Hacker), Michel Slootweg (Information Security Officer - Gemeente Den Haag), René Kroes (Product Owner, I-RE-Al), Saskia Bruines (Wethouder Economie, Internationaal en Dienstverlening - Gemeente Den Haag), Vincent Thiele (CISO - Cybersprint), Wietse Boonstra (Security Researcher, Bug bounty hunter en Hacker).

Laat deze e-guide bijdragen aan het vergroten van de digitale veiligheid in Nederland en daarbuiten. Wij staan open voor vragen en opmerkingen die helpen om onze gezamenlijke inzichten op het gebied van digitale veiligheid door te blijven ontwikkelen.

Jeroen Schipper
CISO gemeente Den Haag

Pieter Jansen
CEO Cybersprint

Den Haag, november 2021

SAMENVATTING

Interne en externe belanghebbenden
Werken aan digitale veiligheid doet u niet vanuit de bekende ‘ivoren toren’. U heeft te maken met verschillende interne en externe belanghebbenden. Deze stakeholders spelen stuk voor stuk een rol in de digitale weerbaarheid van een overheidsorganisatie of commercieel bedrijf. Daarbij is sprake van een persoonlijk belang, eigen verantwoordelijkheden en voorwaarden waaraan moet worden voldaan voordat deze personen een positieve bedrage kunnen leveren aan de gestelde doelen rond digitale veiligheid. In het geval van een gemeente heeft u te maken met bestuurders, verantwoordelijken en medewerkers van de ICT- en security-afdelingen, directeuren en gebruikers van systemen. Voor wat betreft de externe belanghebbenden kunt u zich ook een aantal kritische vragen stellen:

- In hoeverre zijn klanten/burgers zich bewust van het belang van de veiligheid van de systemen waarin hun gegevens worden opgeslagen, verwerkt en gedeeld met andere partijen? En wat verwachten zij op dit vlak van uw organisatie?
- Hoe zit het met leveranciers van diensten en systemen waarvan gebruik wordt gemaakt?
- Hoe betrekt u hackers op een goede manier bij het testen en verbeteren van uw digitale veiligheid?

In hoofdstuk 1 geven we u inzicht in verschillende aspecten die van belang zijn voor interne en externe belanghebbenden.

Organisatieparaatheid
Een organisatie klaarstomen om concrete stappen te zetten op het gebied van digitale veiligheid, raakt aan vele aspecten. Bijvoorbeeld het (her-)organiseren van de security- en de ICT-organisatie en ervoor zorgen dat u beschikt over

voldoende gekwalificeerd personeel vanuit uw eigen organisatie, mogelijk aangevuld met externe expertise in de vorm van inhuur of strategische partners. Een andere bepalende factor is de manier waarop uw organisatie reageert op aanstaande incidenten. Processen die zijn uitgewerkt en beschrijven welke acties nodig zijn in het geval van een op handen (of in uitvoer zijnde) aanval of wanneer een kwetsbaarheid bij u wordt gemeld. Evalueren, vervangen en aanschaffen van benodigde systemen en infrastructuur is weer een ander element. Systemen die u helpen de digitale voetprint en het aanvalsoppervlak van uw organisatie in kaart te brengen, coördinerende tooling die zorgt voor overzicht, inzicht en efficiëntie en bug bounty platformen waarmee u de expertise van hackers in kunt zetten. Connecties leggen met groepen hackers die of in direct contact met uw organisatie of via een bemiddelende partij met regelmaat uw systemen checken op mogelijke kwetsbaarheden. Bij al deze elementen is goede communicatie met interne en externe betrokkenen cruciaal.

Hoofdstuk 2 beschrijft de handvatten om uw organisatie voor te bereiden op de uitvoering van een adequaat beleid voor digitale veiligheid.

Hack-evenement
Zodra digitale veiligheid in de haarvaten zit van uw organisatie, kunt u overwegen om een hack-evenement te organiseren. Hackers gaan daarbij in een gecontroleerde setting in competitieverband op zoek naar mogelijke kwetsbaarheden in uw websites en systemen. Naast een serieuze afweging of een dergelijk evenement waarde toevoegt voor uw organisatie, zijn er tal van andere zaken waar u een besluit over moet nemen:

- Wat is een goede timing om het evenement plaats te laten vinden?
- Wordt het een live evenement of is het online?
- Hoeveel hackers wilt u deel laten nemen?
- Zijn dit alleen professionele hackers of ook studenten?
- Laat u alleen uw eigen systemen hacken of ook die van uw leveranciers?

De meeste aandacht is echter nodig voor de prioritering, opvolging en oplossing van de kwetsbaarheden die gedurende het evenement worden gevonden. De leermomenten uit dit evenement zijn namelijk het belangrijkste ingrediënt om een groei in digitale veiligheid te realiseren.

In hoofdstuk 3 komen deze en andere punten uitgebreid aan de orde. Een draaiboek voor een hack-evenement vindt u in bijlage 1.

Conclusie

De wens om te digitaliseren wordt alsmaar groter en is onlosmakelijk verbonden met aandacht voor digitale veiligheid. Hoe meer processen worden gedigitaliseerd, hoe belangrijker het is om dit veilig te laten verlopen. Zonder adequate informatieveiligheid worden belangrijke systemen onbetrouwbaar en daarmee onbruikbaar. Het goed opzetten van processen en systemen voor digitale veiligheid en het inzetten van hackers kost veel tijd en energie, maar de resultaten zijn altijd positief. Een goede digitale weerbaarheid is uiteindelijk onbetaalbaar omdat het hoge herstelkosten, imagoschade, verlies van klanten en dergelijke kan voorkomen. Door hackers actief te betrekken bij uw beleid voor digitale veiligheid, blijft u criminelen een stap voor.

In dit document wordt gebruikgemaakt van jargon en technische termen. In het Cyberveilig Nederland woordenboek wordt de gebruikte terminologie uitgelegd.

HÂCK THE HAGUE, EEN BEETJE SPANNEND MAAR ONTZETTEND WAARDEVOL

“De samenleving digitaliseert en als gemeente bewegen we daarin mee. Inwoners mogen van een gemeente dezelfde snelheid, service en vernieuwing verwachten. Met veiligheid als randvoorwaarde voor de internationale stad van vrede en recht, staat Den Haag voor goed beschermde ICT-systemen. Daarom laat Den Haag zich jaarlijks hacken door een groot aantal hackers tijdens het evenement Hâck The Hague. Best spannend, maar het levert ontzettend veel inzichten op. Het evenement zorgt jaarlijks voor de nodige bewustwording, binnen maar ook buiten de gemeente. Zo trekt het veel bekijks van inwoners en pers. Een goed signaal, want informatieveiligheid is ontzettend belangrijk. Aan de wedstrijd doen nationale en internationale hackers en studenten mee die allemaal proberen de beveiliging te omzeilen.

Goede voorbereiding en duidelijke spelregels

Hâck The Hague levert andere inzichten op dan een traditionele beveiligingstest. Het vraagt om goede voorbereiding en duidelijke spelregels om ongewenste situaties te voorkomen. Daarom werkt Den Haag nauw samen met experts op dit gebied. Zoals Cybersprint, een van de partners van The Hague Security Delta. Daarnaast moet je als organisatie in staat zijn om de beveiligingslekken die worden gevonden te wegen en zo snel mogelijk te dichten. Het is dus heel belangrijk om er als organisatie ook echt klaar voor te zijn. Dat geldt niet alleen voor de mensen, maar ook voor de processen en de ondersteunende technologie.

Het belang van digitale veiligheid
Voor een bestuurder geeft een evenement als Hâck The Hague extra inzicht in de beveiliging van de systemen. Er wordt met een frisse blik van buiten naar de gemeentelijke ICT gekeken. Maar het levert meer op dan dat. Met de wedstrijd willen we ook studenten enthousiasmeren voor een carrière in cybersecurity. Dat is hard nodig, want de vraag naar cybersecurity-specialisten zal de komende jaren alleen maar toenemen. Een organisatie kan altijd worden gehackt. Daar moet je op voorbereid zijn. Ook voor een cybercrisis moet er een draaiboek klaarliggen. Zo’n crisisplan moet je geregeld oefenen, op alle niveaus – zowel binnen als buiten de organisatie.

Digitale veiligheid is te vaak nog iets wat ‘de ICT-afdeling’ regelt. In werkelijkheid is dit een onderwerp dat op bestuursniveau moet leven en de juiste aandacht moet krijgen. Zonder deze bewustwording is het onmogelijk voor organisaties om op een structurele manier aan digitale veiligheid te werken.

Het thema cybersecurity ontwikkelt zich bij gemeenten steeds verder. In de fysieke wereld is het duidelijk waar de bevoegdheden van een gemeente liggen. In de digitale wereld ligt dat zeker nog niet 100% vast. Daarom bespreken we dit onderwerp ook landelijk binnen de Vereniging Nederlandse Gemeenten (VNG). Onze kennis en ervaring rondom digitale veiligheid en Hâck The Hague is gebundeld in deze e-guide. Ik ben trots op het resultaat: het laat zien dat wij als gemeente Den Haag een echte voorbeeldrol hebben op dit onderwerp. Ik hoop dat het andere gemeenten en organisaties inspireert en motiveert om de volgende stap te zetten.“

Saskia Bruines
Wethouder Economie, Internationaal en Dienstverlening Gemeente Den Haag

HOOFDSTUK 1
INTERNE EN EXTERNE BELANGHEBBENDEN

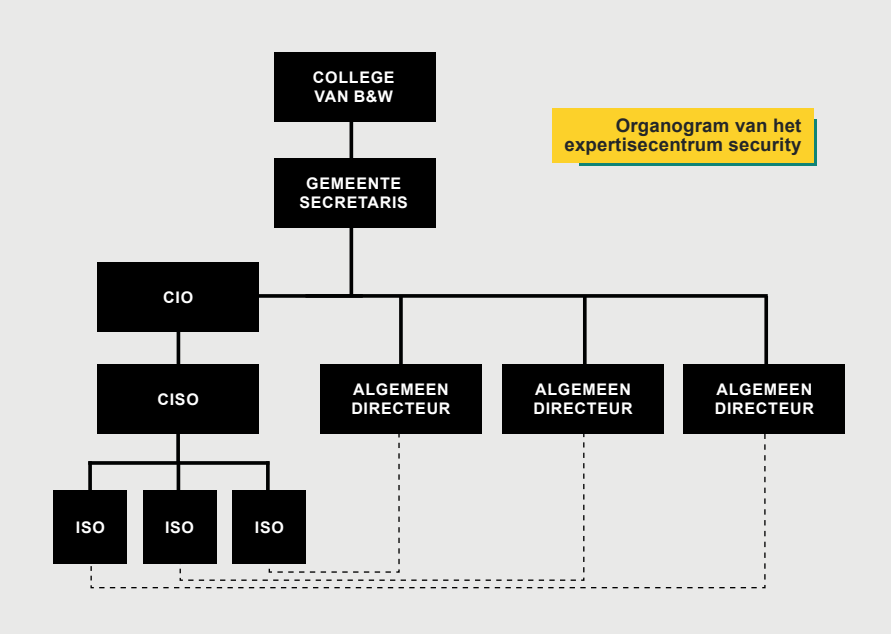
1.1 INTERNE BELANGHEBBENDEN

Bestuurders

Serieus werk maken van de digitale weerbaarheid van een overheidsinstantie of bedrijf, betekent in eerste instantie met de billen bloot durven gaan. Enerzijds omdat u zich wellicht op terrein begeeft waar u zelf minder kennis over heeft en deze van anderen, binnen of buiten uw organisatie, moet betrekken. Anderzijds omdat het confronterend is wanneer blijkt dat de beveiliging van uw producten of diensten toch te wensen overlaat en er investeringen nodig zijn om dit te verbeteren. Sterke overredingskracht en goede argumenten zijn onmisbaar om management en/of bestuur te overtuigen om op eigen initiatief hackers uit te nodigen om systemen te breken. Van nature zijn we als mens geneigd de minder positieve zaken voor onszelf te houden, maar bij digitale veiligheid geldt: hoe opener en transparanter uw aanpak, hoe beter het resultaat.

In de door gemeente Den Haag vastgestelde gemeentelijke doelen is aangegeven dat zorgvuldige omgang met de informatie die de gemeente heeft een belangrijke randvoorwaarde is bij het verder digitaliseren van dienstverlening. Om dit voor elkaar te krijgen zijn voorbeeldgedrag en leiderschap cruciaal. Alleen als iedereen van hoog tot laag in de organisatie door hun eigen gedrag laat zien dat informatieveiligheid belangrijk is, zal dit besef ook bij andere medewerkers ontstaan en zullen zij zich hier ook naar gaan gedragen. Het gehele gemeen-

telijk management ondersteunt en geeft richting aan informatieveiligheid. Het management maakt daarbij een inschatting van het belang dat de verschillende delen van de informatievoorziening voor de gemeente hebben, de risico's die de gemeente hiermee loopt en welke van deze risico's onacceptabel hoog zijn. Op basis hiervan worden acties op het gebied van informatieveiligheid bepaald en wordt de voortgang van de uitvoering bewaakt.



De organisatie van informatieveiligheid vindt plaats op strategisch, tactisch en operationeel niveau die onderling naadloos op elkaar en op de overige processen van de organisatie aansluiten. De verantwoordelijkheid voor de bestuurlijke aansturing binnen gemeente Den Haag ligt bij het college onder leiding van de burgemeester. De dagelijkse uitvoering hiervan ligt bij de gemeentesecretaris. De verantwoordelijkheid voor de inrichting van informatieveiligheid is door de gemeentesecretaris, via de Chief Information Officer (CIO) belegd bij de Chief Information Security Officer (CISO). Het lijnmanagement binnen elke dienst heeft de verantwoordelijkheid om het informatieveiligheidsbeleid uit te voeren onder leiding van de algemeen directeur (AD). De aan de AD toegewezen Information Security Officer (ISO) treedt hierbij op als adviseur van de AD en de sectordirecteuren.

Om informatieveiligheid echt binnen de organisatie in te passen, moet er aandacht zijn voor:

- Processen
- Cultuur, attitude en gedrag
- Organisatie rollen, verantwoordelijkheden en bevoegdheden.

Verantwoordelijken van de ICT- en veiligheidsafdelingen

Chief Information Security Officer (CISO)

De CISO heeft een centrale rol in het beheren van alles dat binnen een gemeente of bedrijf met informatiebeveiliging (middel) en informatieveiligheid (doel) te maken heeft. Het definiëren van standaarden voor het beleid; het analyseren van mogelijke toepassingen van nieuwe ontwikkelingen als het Internet of Things; het bepalen van hoe wordt omgegaan met veranderende wetgeving zoals bijvoorbeeld de BIO en AVG. Jeroen Schipper, CISO van gemeente Den Haag, mede-initiatiefnemer van deze e-guide en onder meer eindverantwoordelijk voor Hâck The Hague, gaat in op de verantwoordelijkheden en voorwaarden om in zijn rol een optimale bijdrage te leveren aan de digitale veiligheid.

(Chief) Information Security Officer

- onafhankelijke positie
- controleren en adviseren
- basiskennis van ICT
- van technisch issue naar impact op de organisatie
- vertrouwensband op niveau

Jeroen: "Als CISO dien je vanuit een onafhankelijke positie te adviseren over informatieveiligheid. Je controleert en adviseert waar het gaat om informatiebeveiligings-maatregelen. De diverse directeuren zijn verantwoordelijk voor het proces en voor onderliggende informatiesystemen. Zij maken uiteindelijk de afweging om een advies al dan niet over te nemen én dragen de consequenties van deze beslissing. Bij de gemeente Den Haag hou ik mij onder andere bezig met het gemeentebrede programma voor informatieveiligheid, waaronder het zorgen voor bewustwording rond digitale veiligheid, overleg met diverse belanghebbenden binnen en buiten de gemeente en regelmatige rapportages om bestuurders besluiten voor te leggen.

Een grote uitdaging bij beleid rond informatieveiligheid, is ervoor zorgen dat de verantwoordelijkheden duidelijk zijn en dat deze ook concreet worden vastgelegd in het beleid. Daarnaast zijn steun, mandaat en verantwoordelijkheid vanuit het management een voorwaarde om in crisissituaties adequaat op te treden.

"Als CISO van gemeente Den Haag zie ik Hâck The Hague eigenlijk een beetje als mijn jaarlijkse beoordelingsgesprek. Wat digitale veiligheid en beveiliging aangaat, kun je beleid maken tot je blauw ziet, maar pas wanneer je een dergelijke evenement opzet, blijkt in de praktijk of wij ons werk naar behoren hebben gedaan."

Jeroen Schipper
CISO gemeente Den Haag

Als CISO, maar ook als ISO, moet je basiskennis hebben van ICT om technische problematieken goed te vertalen naar de potentiële impact op de organisatie. Daarnaast zijn communicatievaardigheden heel belangrijk, evenals een goede vertrouwensband met, in ons geval, dienstdirecteuren. Tenslotte moet je in geval van calamiteiten ook zonder ruggespraak met de organisatie op basis van goede argumenten ingrijpen op systemen of deze zelfs stil durven zetten."

Information Security Manager

Peter van Eijk is Information Security Manager bij Gemeente Den Haag en speelt een belangrijke rol bij het verwezenlijken van de ambities van de gemeente op het vlak van digitale veiligheid. Peter: "Iedere stad heeft een ander cyber security risicoprofiel en kent een andere dynamiek. Daarbij gaat digitalisering bij gemeenten niet alleen over interne systemen, maar ook over digitalisering in de stad zelf. Dit gaat steeds verder, wat ook meer cybersecurity risico's met zich meebrengt. Binnen onze gemeente is er veel aandacht voor het vergroten van onze weerbaarheid. Alleen fysieke veiligheid is natuurlijk niet genoeg; juist ongrijpbare, digitale risico's willen we beperken door ze inzichtelijk te maken, te analyseren, te prioriteren en zo snel mogelijk te verlagen of het liefst helemaal op te lossen. Voorwaarden om dit goed te kunnen doen, is het op orde hebben van je interne huishouding, goede communicatie en een goede vertrouwensband met de personen met wie je moet schakelen.

> "In control zijn betekent niet dat je elke kwetsbaarheid direct moet repareren. Het gaat over inzicht hebben in de kwetsbaarheden en hun mogelijke impact, waardoor je een goede afweging kunt maken of je iets nu of later aanpakt."
>
> *Peter van Eijk*
> *Information Security Manager - gemeente Den Haag*

In mijn rol geef ik richting en sturing aan de afdeling ICT Security op strategisch en tactisch niveau, met als doel tactische doelstellingen te realiseren. Samen met mijn team zorg ik voor de technische inhoud, adviseren we C-level management en dragen we bij aan de ontwikkeling en actualisering van de informatieveiligheidsstrategie en -beleidsplannen van de gemeente Den Haag. Als verantwoordelijke en medewerker van de security-afdeling heb je een groot verantwoordelijkheidsgevoel, betrokkenheid en interesse in de materie nodig. Met een 9 tot 5 mentaliteit ga je het in dit vakgebied echt niet redden.

Mijn advies is: denk groot, maar begin klein. Start met een beperkte scope: hoe lopen interne processen, zijn alle assets geregistreerd. Kijk wat werkt en wat

niet en breidt het langzaam uit. Met beschikbare technologie kun je de hele wereld scannen, maar dan komt er zóveel informatie terug dat het niet te handelen is. Betrek medewerkers bij wat je doet, ICT’ers én mensen uit de organisatie. Zij moeten aan de slag met het oplossen van de kwetsbaarheden. Hoe sneller zij stappen ondernemen, hoe minder ze hoeven op te lossen. Door de positieve effecten van onze inspanningen inzichtelijk te maken, hopen we mensen uiteindelijk zover te krijgen dat ze zelf mee gaan denken en risico’s aanpakken voor het problemen worden.”

Dienstdirecteuren en gebruikers van systemen

Een goede en veilige digitale dienstverlening is en blijft een belangrijk punt van aandacht. Het is echter niet alleen de verantwoordelijkheid voor bestuurders en managers van essentiële afdelingen als ICT en Security, maar eigenlijk voor alle medewerkers binnen een organisatie of bedrijf. Ook binnen een gemeente zijn directeuren én gebruikers van systemen een cruciale schakel bij het goed en veilig omgaan met informatie van henzelf en derden. Borging van digitale veiligheid binnen de organisatie is heel belangrijk. Om gevonden kwetsbaarheden op te kunnen lossen, moet je weten wie verantwoordelijk is voor de verschillende applicaties en websites. In niet alle gevallen is dat echter duidelijk. En is de eigenaar eenmaal gevonden, dan is het nog een uitdaging om deze mensen te overtuigen van de noodzaak om actie te ondernemen of intern urgentie te krijgen om een aanpassing met spoed door het proces te krijgen.

De rol van de directeuren binnen de gemeente is al beschreven onder het kopje ‘bestuurders’, maar uiteindelijk moeten alle medewerkers de juiste instelling hebben ten aanzien van digitale veiligheid. Houding en gedrag ten aanzien van digitale veiligheid zullen daarom regelmatig door middel van bewustwordingscampagnes en -trainingen moeten worden beïnvloed. Betrokkenen bewust maken en houden van het belang van informatieveiligheid zorgt ervoor dat zij hun eigen rol daarin kunnen vervullen. Op deze manier wordt het juiste gedrag bevorderd en ontstaat er een cultuur waarin men elkaar daadwerkelijk durft aan te spreken op gedrag. Genoemde campagnes en trainingen worden binnen gemeente Den Haag georganiseerd vanuit de CISO, maar het is de verantwoordelijkheid van elke manager om ervoor te zorgen en erop toe te zien dat al zijn of haar medewerkers hier serieus aan meedoen. Gezien de overlap met het onderwerp privacy/gegevensbescherming dat onder verantwoordelijkheid valt van de functionaris gegevensbescherming, zal de bewustwording over dit onderwerp en die van informatieveiligheid vaak in combinatie worden georganiseerd. Naast de permanente en verplichte educatie wordt vanuit de CISO en ISO’s door middel van evenementen en publicaties gezorgd voor continue aandacht voor het onderwerp.

1.2 EXTERNE BELANGHEBBENDEN

Burgers

Als we kijken naar de omgeving waarin een Nederlandse gemeente opereert, dan zijn daar allereerst de burgers. Zij zijn de voornaamste klanten van de gemeenten en hebben er belang bij dat de vaak gevoelige informatie die met uiteenlopende gemeenteloketten wordt gedeeld, op een veilige manier wordt verwerkt en opgeslagen. Daarnaast hebben zij ook hun eigen verantwoordelijkheid als het gaat om een stuk digitale veiligheid. Maar wat weten de burgers in de gemeente eigenlijk van cybersecurity? En wat verwachten ze op dit vlak van een gemeente? We vragen het aan Daan Rijnders, Lead (Kwartiermaker) Cyber Secure bij gemeente Den Haag.

Daan: “In de samenleving lijkt steeds meer aandacht te komen voor digitale veiligheid. Dat is terecht en belangrijk. Alleen worden er, bijvoorbeeld in de media, wel veel verschillende termen gebruikt. Denk aan cybersecurity, cyber crime, cyber resilience en allerlei soorten incidenten zoals ransomware, phishing, DDoS-aanvallen en malware. Het gebruik van termen die stuk voor stuk net een andere invalshoek en doelgroep hebben, maakt het extra verwarrend. Door het gebruik van Engelse woorden klinkt het voor inwoners vaak ook spannender en vooral moeilijker dan het eigenlijk is. Daardoor denken mensen soms onterecht dat ze zelf niets aan digitale veiligheid kunnen doen of dat ze geen kans maken om slachtoffer te worden.

Gelukkig zijn er goede nationale initiatieven die helpen om burgers en bedrijven beter te informeren, zoals Alert Online, veiliginternetten.nl en de hackhelpdesk.nl. In Den Haag werken we met het project ‘Digitaal Veilig in de Wijk’ samen met de politie en inwoners aan het verhogen van de digitale weerbaarheid in de wijk. Burgers en ondernemers worden door ons getraind en zetten zich als Digitaal Ambassadeur vrijwillig in om hun buurtbewoners bewust te maken van de risico’s op het gebied van digitale veiligheid. Ook Hâck The Hague heeft de afgelopen jaren bijgedragen aan een groeiend bewustzijn over digitale veiligheid bij de burgers en bedrijven van onze gemeente. Digitale veiligheid is vaak moeilijk tastbaar, maar het wordt opeens heel mooi zichtbaar als er een paar honderd hackers live bezig zijn in het Atrium van het stadhuis, terwijl de inwoners staan te wachten om een paspoort op te halen. Dan krijg je vanzelf het gesprek dat we met elkaar moeten hebben.”

Leveranciers

Net als bij burgers zal ook het kennisniveau van leveranciers van systemen en applicaties verschillen. Zij vormen een belangrijk onderdeel van het (digitale)

ecosysteem van een gemeente of bedrijf en daarom wilt u hen zeker betrekken bij activiteiten en initiatieven om uw digitale veiligheid te verhogen. Michel Slootweg, een van de ISO’s van gemeente Den Haag, is bij Hâck The Hague aanspreekpunt van leveranciers en helpt hen om goed voorbereid aan het evenement deel te nemen.

Michel: “Als gemeente begrijpen wij dat het voor veel leveranciers die voor het eerst aan Hâck The Hague deelnemen spannend is om hun systemen open te stellen voor hackers. Maar de ervaring leert dat de inzichten die tijdens de wedstrijd naar voren komen, heel relevant voor hen zijn en voor vele bedrijven de opmaat betekenen naar een (nog) betere digitale veiligheid van hun systemen en websites. Daarnaast werken we er als gemeente aan om de begeleiding van leveranciers elk jaar weer te verbeteren. Dat doen we onder andere door het delen van informatie en het beschikbaar stellen van tools waarmee leveranciers voorafgaand aan het hack-evenement gratis hun te testen omgevingen alvast een keer kunnen scannen. Op die manier zorgen zij ervoor dat de eenvoudig te verhelpen kwetsbaarheden worden opgelost vóórdat de deelnemende hackers de aanval op hun systemen inzetten.”

Hoe is het om als leverancier van gemeente Den Haag deel te nemen aan Hâck The Hague? Twee bedrijven die één of meerdere edities van deze hack-wedstrijd hebben meegemaakt, delen desgevraagd de ervaringen van hun deelname.

DG Groep - Dataveiligheid is nu echt geborgd in onze bedrijfsprocessen
DG Groep heeft in 2019 meegedaan aan Hâck The Hague met hun applicatie GISIB online. Met deze applicatie worden alle assets oftewel kapitaalgoederen van de overheid geregistreerd, geïnspecteerd en gemanaged. Daarbij kunt u denken aan wegen, lantaarnpalen, maar ook zaken als gras, bos, oevers en riet. Een gemeente streeft ernaar een zo hoog mogelijke kwaliteit product te leveren aan haar burgers en GISIB online helpt hen daarbij. Frank Jan Uittenbogaart, Directeur/manager product development van het bedrijf, zegt het volgende over het belang van digitale veiligheid en de voordelen die deelname aan Hâck The Hague met zich meebrengt.

Frank Jan: “Informatieveiligheid is een hot topic, en terecht. We hebben tegenwoordig allemaal te maken met spam en spoofing en rare mailtjes van banken die geen banken blijken te zijn. Ons eigen systeem, GISIB online, bevat een grote hoeveelheid data die moet worden beveiligd tegen ongeoorloofd gebruik, ook al is 80-90% van die gegevens gewoon openbaar beschikbaar. Als ICT-leverancier moet je je terdege beseffen dat we zonder adequate informatieveilig-

heid over 20 jaar helemaal nergens meer zijn met onze ICT. Als belangrijke systemen onbetrouwbaar worden omdat ze met regelmaat niet bereikbaar zijn of niet doen wat ze moeten doen, hebben we er niets meer aan. Hâck The Hague is een uniek evenement in Nederland met een groot educatief aspect. Het heeft ons geholpen om de bewustwording rond digitale veiligheid binnen ons bedrijf goed op de kaart te zetten.

Onze eerste deelname aan Hâck The Hague in 2019 was best spannend, je legt tenslotte moedwillig je eigen software op de 'pijnbank'. We hadden ons systeem natuurlijk naar beste eer en geweten beveiligd, maar je hebt geen idee of dat genoeg is wanneer er meer dan 100 hackers op je af worden gestuurd. Aangezien we zelf geen expert zijn in het beveiligen van data, hadden we ter voorbereiding externe hulp ingeroepen om alles vooraf nog een keer te doorlopen. Tijdens Hâck The Hague zijn een aantal dingen boven tafel gekomen. Onder andere security headers op de website die niet volledig veilig waren waardoor informatie kon lekken. Dit was vrij eenvoudig op te lossen en dat is ook ter plekke gebeurd. Een andere gevonden kwetsbaarheid zat in de software zelf en werd direct doorgezet naar het developmentteam dat in korte tijd een patch heeft uitgebracht waarmee het probleem werd opgelost. Met de hacker die het probleem aan het licht bracht, ontstond een leuke dialoog en hij heeft op eigen initiatief de opgeleverde patch gecheckt om

SUPPLY CHAIN HACKS, EEN GEZAMENLIJKE VERANTWOORDELIJKHEID

Bij de woorden 'supply chain', ofwel leveranciersketen, legt u misschien in eerste instantie de link met logistiek, maar ook in de wereld van cyberveiligheid is het de laatste tijd een 'hot topic'. In de ICT supply chain vinden namelijk recentelijk de meest impactvolle hacks plaats. Vincent Thiele, CISO bij Cybersprint, legt uit wat het fenomeen supply chain hacks inhoudt en waarom een optimale digitale beveiliging vraagt om samenwerking met een zo breed mogelijke groep van partijen waarmee u samenwerkt.

Wat is het

Vincent: "Een traditionele supply chain gaat over alle schakels die nodig zijn om een product van grondstof naar consument te krijgen. ICT heeft een eigen supply chain, namelijk alles wat nodig is om een goede ICT-dienstverlening te realiseren. Of het nu gaat om een gemeente of een commercieel bedrijf, in beide gevallen zijn er allerlei toeleveranciers betrokken bij de dienstverlening aan de burger of klant. Denk hier bijvoorbeeld aan mailservers, of softwareprogramma's voor het afhandelen van een (klant-)vraag. Bij een supply chain hack komen criminelen via één van deze poorten binnen waarna zij grote delen van systemen lam kunnen leggen of in gijzeling kunnen nemen. Supply chain hacks zijn een relatief nieuw fenomeen waarover nog veel vragen onbeantwoord zijn. Het is in elk geval belangrijk om te weten dat er drie verschillende soorten ICT supply chains bestaan, ieder met hun eigen risico's:

- Bij een hardware supply chain hack kunnen bijvoorbeeld door gebruik van chips van een specifieke leverancier elementen in hardware producten van anderen worden geïntroduceerd met allerlei mogelijke ongewenste gevolgen van dien.
- Software supply chain hacks kunnen worden veroorzaakt door het kleinste stukje software dat u van een derde partij betrekt, die stiekem kan worden meegevoerd in een software-update van deze partij. Hiermee zijn de ontwikkelaars van dit stukje onbetekenende software in staat toegang te krijgen tot verschillende systemen binnen uw organisatie, zoals recentelijk het geval was bij de incidenten via Citrix, SolarWinds en Microsoft Exchange.
- Een infrastructuur supply chain hack wordt gedaan via kanalen die ICT service providers gebruiken om service updates uit te voeren van de infrastructuur van uw organisatie.

Wij hebben de verschillende typen supply chain hacks uitgebreider beschreven in een editorial over dit onderwerp, inclusief de oplossingen voor deze risico's."

Wie loopt risico

"Mocht u van mening zijn dat uw ICT supply chain te beperkt is om enig risico te lopen, dan moet ik u helaas uit de droom

helpen. Élke organisatie die software, hardware of ICT-dienstverlening inkoopt van derden, voor eigen gebruik of ter verwerking in eigen producten, kan slachtoffer worden van een supply chain hack. En geen enkele organisatie maakt 100% van hun hardware en software zelf. Het simpele downloaden van een publiekelijk beschikbare plug-in om de performance van uw website te monitoren, kan het Trojaanse paard zijn waarmee u criminelen onbewust en onbedoeld toegang geeft tot het hart van uw organisatie.

Het zijn ook vaak niet de minste organisaties waarvan systemen en/of software besmet blijken te zijn. Recente voorbeelden van impactvolle supply chain hacks waren bijvoorbeeld Kaseya, een dienstverlener die voor vele bedrijven beveiligingsdiensten verleende en SolarWinds, een veel gebruikte suite van programma's om ICT-infrastructuren te beheren."

Wat kunt u doen?

"Supply chain attacks lijken steeds meer voor te komen en op dit moment is er nog geen eenduidige oplossing voorhanden. Ook bij dit onderwerp geldt dat het belangrijk is dat u zelf goed op de hoogte bent van de hardware en software waar uw organisatie gebruik van maakt. Dat u zich bewust bent van de risico's die dit met zich mee kan brengen en direct kunt handelen wanneer er daadwerkelijk iets misgaat. Mocht één van uw derde partijen namelijk toch besmet zijn, dan telt iedere seconde. Als er eerst nog gezocht moet worden wáár die stukjes software precies draaien, duurt het alleen maar langer voor er aan een oplossing kan worden gewerkt.

Zorg er daarnaast voor dat de toeleveranciers waarmee u werkt eenzelfde beveiligingsniveau nastreven als uzelf. Afgezaagd cliché of niet, maar ook uw digitale beveiliging is zo sterk als de zwakste schakel. Zie erop toe dat u afspraken over te nemen beveiligingsmaatregelen eenduidig en transparant vastlegt in uw inkoop- en/of aansluitingsvoorwaarden. Vergeet ook niet de naleving van deze afspraken actief te controleren zodat duidelijk is dat het om meer gaat dan een formaliteit.

Bij Cybersprint monitoren we onze omgeving en die van onze klanten intensief en we houden daarbij de mogelijke impact van derden nauwlettend in de gaten. Wij zien het als een mogelijkheid om samen te werken met partners en toeleveranciers. Wanneer we een kwetsbaarheid in het aanvalsoppervlak van een leverancier vinden, gaan we in gesprek om dat probleem op te lossen. Hier worden beide partijen veiliger van.

Gemeente Den Haag doet hetzelfde. Hâck the Hague is hiervan een klein maar sprekend voorbeeld, waarbij zowel de systemen van de gemeente zelf als die van een groot aantal van haar toeleveranciers worden getest op hun digitale veiligheid. Door deze derde partijen bij het evenement te betrekken, wordt het onderzoeksgebied – en de positieve effecten ervan – vele malen groter. Het is één van de manieren waarbij we elkaar helpen naar een hoger beveiligingsniveau."

te kijken of de oplossing inderdaad afdoende was.

Kort na onze deelname aan Hâck The Hague in 2019 deden we mee aan een aanbesteding waarbij een van de eisen was dat wij ISO 27001/2 gecertificeerd waren. Op dat moment waren we dubbel blij dat we met onze deelname aan Hâck The Hague het traject van databeveiliging al hadden ingezet. Het was zeg maar een soort opmaat - nu zijn er standaard periodieke controles van de eigen bedrijfsvoering en kwaliteit van onze softwareontwikkeling en is dataveiligheid een vast onderdeel van onze bedrijfsprocessen. Ik kan alle leveranciers van gemeente Den Haag dan ook van harte aanbevelen om vooral mee te doen aan Hâck The Hague. Door samen te werken met hackers, brengen we elkaar telkens naar een hoger niveau. Zij helpen ons als leverancier om de krochten van het domein te onderzoeken en daarmee mogelijke zwakheden boven tafel te krijgen voordat kwaadwillenden dit doen. Heeft u geen kennis van het domein van dataveiligheid? Neem dan een specialist in de arm voor goed advies, maar laat u vooral niet weerhouden van deelname aan Hâck The Hague, want dat is gewoon heel waardevol."

I-REAL - Hâck The Hague helpt ons om digitale veiligheid naar een hoger niveau te krijgen

I-REAL creëert het Internet of Things voor de publieke sector door beheerders toegang te geven tot objecten die bijdragen aan de afvoer van water.

Hun product, I-REALM2M, wordt ook ingezet door de gemeente Den Haag om elementen in de waterketen en de publieke infrastructuur te monitoren, controleren en administreren. René Kroes, Product Owner bij I-REAL geeft aan waarom Hâck The Hague een welkome aanvulling is op de activiteiten die zij ondernemen om de veiligheid van hun software te verbeteren.

René: “Onze software helpt gemeenten om hun water en publieke infrastructuur te managen en objecten als fonteinen, bruggen en beweegbare afsluitingen te besturen. U kunt zich waarschijnlijk voorstellen wat het betekent als iemand onze software hackt en de controle over deze dingen overneemt. Daarom is digitale veiligheid altijd al een belangrijk aandachtsgebied geweest binnen ons bedrijf. Behalve onze deelname aan Hâck The Hague voeren we zelf regelmatig pentesten en andere activiteiten uit om onze ISO-certificering up-to-date te houden. Gemeenten verwachten van ons dat we een waterdichte oplossing leveren en dat is tot nu toe nog altijd gelukt.

Onze software is altijd in ontwikkeling, waarbij we telkens de afweging maken tussen de mate van toegankelijkheid van de software en het behoud van de nodige veiligheidsniveaus. Hâck The Hague is een van de manieren waarop we testen of we hier succesvol in zijn. We hebben liever dat een deelnemer aan dit evenement een kwetsbaarheid ontdekt in een van onze producten dan dat we zonder het te weten de deur open hebben staan voor onbekenden die het minder goed met ons voorhebben. Natuurlijk is het niet fijn wanneer er een grote bug in je systeem wordt gevonden, maar dat geeft je wel een kans om het op te lossen. Deelname aan Hâck The Hague laat zien dat je digitale veiligheid serieus neemt en dat je werkt met experts op dit gebied om je producten te verbeteren.”

Hackers

Voor veel mensen staat de term ‘hacker’ nog steeds gelijk aan duistere figuren die aan de rand van de maatschappij bezig zijn met het uitvoeren van criminele activiteiten. Onterecht. Het zijn juist de hackers die ervoor zorgen dat meer of minder impactvolle kwetsbaarheden tijdig worden gesignaleerd bij de eigenaars van de producten zodat zij maatregelen kunnen nemen vóór iemand hier misbruik van kan maken. Natuurlijk speelt daarbij mee dat hackers in veel gevallen geld verdienen aan het aanmelden van kwetsbaarheden. Maar de belangrijkste reden voor veel van hen is dat zij op die manier concreet bijdragen aan het verbeteren van de digitale veiligheid.

Criminele hackers proberen continu in te breken bij organisaties zoals de Gemeente Den Haag. Wanneer een nieuw gemeentelijk systeem op het internet wordt aangesloten, duurt het vaak slechts 2 minuten voordat een eerste aanval-

spoging wordt gedaan. Dit zijn over het algemeen niet de hackers waar u graag mee samen wilt werken. Ethische hackers daarentegen zijn 'een ander soort': zij proberen binnen te komen in systemen met als doel applicaties en websites veiliger maken. Deze hackers houden zich aan de spelregels en melden gevonden kwetsbaarheden bij de betreffende organisatie om te voorkomen dat deze wellicht misbruikt worden door kwaadwillende personen. Maar hoe zitten deze hackers zelf in de wedstrijd en welke verantwoordelijkheden zien zij voor zichzelf in het kader van digitale veiligheid? We leggen deze vragen voor aan een tweetal actieve hackers: Jonathan Bouman en Wietse Boonstra.

Jonathan Bouman combineert het beroep van huisarts met die van hacker. Tijdens zijn studie geneeskunde heeft hij veel geprogrammeerd en was hij vanuit dat werk actief bezig met het beveiligen van persoonsgegevens. Later als huisarts zag hij het belang van een goede beveiliging van digitale medische en persoonlijke gegevens van zijn patiënten. Door actief te zijn als hacker en zijn kennis over digitale veiligheid te delen, levert hij hier een positieve bijdrage aan.

Wietse Boonstra is al jarenlang actief als security researcher, bug bounty hunter en hacker. Hij is onder andere bekend van de door hem ontdekte Kaseya kwetsbaarheid die wereldwijd impact had. Wietse is vanaf jongs af aan bezig met digitale veiligheid; in eerste instantie als hardware hacker en later door 'alles wat hij tegenkomt op het internet te testen op kwetsbaarheden'. Hij rapporteert (potentiële) issues die hij tegenkomt bij de eigenaren, "omdat niemand er wat aan heeft als gegevens op straat liggen en bedrijven hierdoor over de kop gaan."

Wat is het belang van digitale veiligheid volgens jou en wordt hier voldoende aan gedaan door bedrijven?

Jonathan: "Mijn werk als huisarts is gebaseerd op vertrouwen tussen patiënt en arts. Alleen als ik dat vertrouwen heb, kan ik mijn werk doen. Op mijn beurt moet ik kunnen rekenen op de veiligheid van de computer waarin ik alles in vastleg. Een principe dat geldt voor de hele zorg. Digitale veiligheid ligt mij dus na aan het hart en ik draag graag mijn steentje bij. In principe hebben alle systemen grote of kleinere kwetsbaarheden. Het is ook helemaal niet erg dat iets lek is, maar wordt een kwetsbaarheid geconstateerd, dan moet het wel snel oplossen. De enige manier om dat te doen is kennis delen, het probleem oplossen en zorgen dat alles zo snel mogelijk weer veilig is. Samen ben je sterker, ook als je een vuist wilt maken tegen cyber crime. Deel kennis, laat de community in teamverband voor je werken, zorg voor kruisbestuiving. Als uw medewerkers eenmaal kennis hebben gemaakt met hackers en daar open en transparant mee omgaan, weten zij elkaar ook makkelijker te vinden wanneer het nodig is."

Wietse: "Alles is digitaal tegenwoordig dus daar moet je rekening mee houden. Als bedrijf, maar zeker ook als privépersoon. Als uw wachtwoord voor uw mailbox niet veilig is en u hebt ooit een keer een kopie van uw paspoort per mail verstuurd bijvoorbeeld, dan kan een crimineel hier heel eenvoudig bijkomen en kan hij zich vervolgens zonder problemen online voor u uitgeven. Kijk naar de hack

bij Het Hof van Twente, veroorzaakt door een te simpel wachtwoord. Natuurlijk snap ik hoe het gebeurt, maar bedenk dat een crimineel nooit aan de voordeur komt rammelen, maar achterom komt om te kijken of er een raampje openstaat. Dat geldt ook online. Iedereen moet een beetje gaan denken als een crimineel en als bedrijf moet u er in elk geval voor zorgen dat digitale veiligheid voor strategische zaken goed geregeld is. Daarmee kunt u veel ellende voorkomen. Het is alleen een uitdaging om kwalitatief goede hackers te vinden: doet u dat zelf, via een platform etc. Er is helaas nog geen sprake van een goede, overkoepelende certificering van hackers."

Welke verantwoordelijkheden heb jij als hacker?
Jonathan: "Als ik een lek vind, dan weet ik tot hoever ik kan gaan. Meestal kun je meerdere kleine gevonden kwetsbaarheid combineren om een groter lek te vinden. Je bent ook als hacker altijd op zoek naar een juiste balans, wanneer is de gevonden fout relevant genoeg om te melden en waar moet ik verder zoeken om de impact duidelijk te maken. Door bedrijven te informeren over vervolgstappen die ikzelf zou ondernemen, kunnen zij ervoor zorgen dat gevonden kwetsbaarheden goed en volledig worden verholpen."

Wietse: "Voor mij ligt de grens als hacker bij het aan de haal gaan met data waar je door een kwetsbaarheid toegang toe krijgt. Als je bijvoorbeeld bij een grote verzekeringsmaatschappij een dump zou kunnen maken van hun database, dan geef je dat aan hen door en daar blijft het bij. Als je met een code een bepaald systeem binnen kunt komen, dan kies je de minst schadelijke code om aan de eigenaar van het systeem aan te tonen dat er een lek is dat gefikst moet worden. Je gaat nooit zover dat je een systeem platlegt, op welke manier dan ook".

Wat heeft een hacker nodig om een goede job te kunnen doen?
Jonathan: "Mijn tip voor organisaties die samen willen werken met hackers is om een relatie met hen op te bouwen. Hou hackers geïnformeerd over de kwetsbaarheden die ze aanleveren. Door hackers te betrekken bij wat u doet, wordt de motivatie groter om bijdragen aan de veiligheid van uw bedrijf te blijven leveren. Deel opgeloste kwetsbaarheden zodat anderen ervan kunnen leren en stel hen op die manier in staat om (nog) effectiever op zoek te gaan naar gaten die gedicht moeten worden. Durf kennis te delen - dat geldt zowel voor hackers als voor bedrijven. Als u kennis voor uzelf houdt, dan helpt u niet het internet veiliger te maken. Deel kennis zodra dat mogelijk is en zorg voor een veilige omgeving waar hackers hun werk kunnen doen."

Wietse: "Elk bedrijf heeft er baat bij wanneer hackers meekijken met de beveiliging van de organisatie. Zorg er daarom voor dat u duidelijke regels vaststelt

al dan niet in de vorm van een Coordinated Vulnerability Disclosure, op basis waarvan u hackers in de gelegenheid stelt op een goede manier een bijdrage hieraan te leveren. Ik denk dat het belangrijk is dat de beloning die je krijgt voor een gemelde hack, past bij de waarde ervan voor de organisatie. Je meldt een kwetsbaarheid niet zomaar, je maakt een organisatie toch weer wat veiliger en dan is het wel zo prettig dat je er iets voor terug krijgt waar je zelf iets voor kunt kopen - je moet als hacker tenslotte ook kunnen leven.”

HOOFDSTUK 2
VOORBEREIDING INTERNE ORGANISATIE

Om als bedrijf of overheidsinstelling serieus aan de slag te gaan met digitale weerbaarheid, moeten eerst de voorwaarden worden gecreëerd om dit daadwerkelijk te kunnen realiseren. Iedereen moet zich bewust zijn van hun eigen verantwoordelijkheden en wat zij zelf kunnen doen om de weerbaarheid te vergroten. Zij moeten hiervoor beschikken over de nodige kennis, capaciteit en middelen. Een ander aandachtspunt is de onderlinge samenwerking tussen de afdelingen, want alleen samen maak je je echt sterk tegen ongewenste digitale aanvallen en kunt u datalekken voorkomen. Ook moderne en adequaat ingezette ICT-systemen en -infrastructuur liggen aan de basis van digitale veiligheid. Net als goed geborgde processen voor ICT en vulnerability management. Nauwe samenwerking met een bij uw organisatie passende hacker-community is de kers op de taart van de continue monitoring en verbetering van uw digitale veiligheid. In dit hoofdstuk worden deze onderwerpen in meer detail uitgewerkt.

> *Cybersecurity doe je niet alleen,*
> *het is een gezamenlijke verantwoordelijkheid*

2.1 INTERNE AFDELINGEN

Alle afdelingen van een organisatie spelen een rol waar het gaat om digitale veiligheid. Bij een gemeente moet elke dienst of departement ervoor zorgen dat zij op een bewuste manier omgaat met (het beschermen van) gevoelige infor-

matie. En websites, systemen en applicaties zodanig beveiligen dat de kans op misbruik minimaal is. Twee disciplines in het bijzonder zijn bepalend voor de operationele kant van digitale veiligheid van uw organisatie: security en ICT. Met een goede samenwerking tussen deze twee disciplines zorgt u ervoor dat technische risico's tijdig worden gesignaleerd, op een passende manier worden vertaald naar potentieel risico en waar nodig op een adequate manier en binnen een passende doorlooptijd worden opgelost.

Security-organisatie

Het is in deze e-guide al een paar keer ter sprake gekomen: digitale veiligheid en informatieveiligheid worden steeds belangrijker. Enerzijds door de wens om altijd en overal gebruik te maken van diensten en producten wat resulteert in een alsmaar grotere wordende vraag naar digitale dienstverlening. Anderzijds door onze groeiende afhankelijkheid van digitale informatievoorziening. (Nieuwe) wet- en regelgeving bepalen daarbij in grote mate hoe overheid en bedrijven invulling moeten geven aan de veiligheid van hun systemen en informatie.

Security-afdeling: Voorwaarden om goed te functioneren

- Beschreven rollen en verantwoordelijkheden (wie doet wat in het kader van digitale veiligheid).
- Duidelijk beleid dat op strategisch, tactisch en operationeel niveau in de organisatie is belegd.
- Actieve controle op naleving van de afspraken.
- Bereidheid om samen te werken aan een optimale bescherming

De security-organisatie met aan het hoofd de Chief Information Security Officer (CISO), wordt geacht om met een deugdelijk pakket aan maatregelen te komen die de vertrouwelijkheid, integriteit en beschikbaarheid van informatie binnen een bedrijf of overheidsinstelling waarborgt. Er kan alleen sprake zijn van een succesvol beleid rond digitale veiligheid en informatieveiligheid wanneer maatregelen en voorschriften op strategisch, tactisch en operationeel niveau in de organisatie zijn verankerd. Dat betekent dat iedereen in de organisatie weet wat er van hem/haar wordt verwacht en dat de voorwaarden om de juiste dingen te doen, zijn ingevuld. Daarnaast dient er controle te zijn op naleving van de afspraken, waarbij personen actief worden aangesproken op mogelijke verbeterpunten. Een open, transparante communicatie houdt personen continu betrokken en geïnformeerd. Zeker (maar niet alleen!) in het geval van een noodsituatie.

De security-organisatie, specifiek in de persoon van de Information Security Officer (ISO), zorgt ervoor dat de potentiële (technische) risico's worden vertaald naar risico's voor de organisatie. Dat gebeurt nadat in samenspraak met ICT is bepaald welke data en systemen mogelijk worden bedreigd en hoe groot de waarschijnlijkheid en de impact daarvan zijn. In het geval van een gemeente

Digitale veiligheid regel je niet op kantoordagen van 9 tot 5. Het vraagt om onafgebroken betrokkenheid, processen die kloppen en een basis die op orde is.

is de ISO zó goed op de hoogte van de belangen van de dienst waarvoor hij werkt, dat hij het gevonden (technische) risico in de juiste context kan plaatsen en weet welke systemen en onderdelen van de infrastructuur mogelijk gevaarlopen. Op basis van deze informatie kan de ISO de directeur van de dienst informeren over de mogelijke implicaties van het gevonden risico en adviseren welke maatregelen het best kunnen worden genomen. Daarmee zorgt de ISO ervoor dat de betreffende directeur een goed gefundeerde beslissing kan nemen over de te ondernemen acties.

Voor een adequate invulling van haar rol is de security-afdeling afhankelijk van de beschikbare kennis, ervaring en benodigde tools/middelen waarover zij beschikt. Daarnaast is de kwaliteit van de informatie die zij krijgt aangeleverd een bepalende factor. Wat is de precieze kwetsbaarheid, in welk systeem is deze gevonden, wat zijn de technische implicaties en welke diensten maken gebruik van deze systemen? Om goed te functioneren, heeft de security-afdeling de back-up van het management nodig en moet zij beschikken over voldoende mandaat om bij calamiteiten snel en goed te kunnen handelen.

Security gaat over zoveel meer dan kaders, beleid en controle. Inzicht in implicaties van technische risico's, kennis van processen van een afdeling of dienst, goede en tijdige communicatie en onderling vertrouwen zijn minstens zo belangrijk voor het realiseren van een adequate (digitale) veiligheid.

ICT-organisatie

Om de security-afdeling van voldoende en kwalitatief goede informatie te voorzien over mogelijke veiligheidsrisico's, moet de ICT-afdeling beschikken over een heel breed scala aan (vaak specialistische) kennis, ervaring en ondersteunende tools. Ook bij ICT is het belangrijk om nooit uit het oog te verliezen dat digitale veiligheid geen 'ICT-ding' is, maar de zorg van een hele organisatie. Daarnaast is digitale veiligheid geen tijdelijk project, maar een permanente dagelijkse taak. De inzet van ICT ondersteunt bij het implementeren van het veiligheidsbeleid ten behoeve van de continuïteit van de organisatie. Diverse tools kunnen u helpen om continue te toetsen hoe u ervoor staat qua aanvalsoppervlakte, welke risico's u loopt en welke mogelijkheden tot uw beschikking staan

om deze te mitigeren. Mensen, processen en technologie zijn de drie elementen die bepalen of uw ICT-afdeling haar basis op orde heeft. De mate waarin u deze elementen in kunt zetten, wordt bepaald op basis van de middelen die u hiervoor ter beschikking kunt stellen versus de mate van risicobereidheid.

Het komt zelden voor dat een organisatie zelf beschikt over alle benodigde expertises die nodig zijn op het gebied van digitale veiligheid. Kijkend naar het element **'mensen'**, dan kunt u zich als eerste de vraag stellen of u de benodigde specialisten zelf in huis heeft of haalt, of dat u deze tijdelijk betrekt van derden. Meestal wordt het uiteindelijk een mix van beide, in een verhouding die voor iedere organisatie anders is. Gemeente Den Haag wordt ondersteund door diverse partijen met specialistische kennis op het gebied van technologie en digitale veiligheid. Bij de selectie van deze partijen kijken we niet alleen naar de kwaliteit van de geleverde oplossingen of dienstverlening, maar vooral ook naar de bereidheid om samen met ons de fases van de zogenaamde cybersecurity journey te doorlopen. De mate waarin wij als gelijke partners samenwerken met derden en in hoeverre sprake is van complementaire kennis en kunde, bepalen het verschil dat we maken voor de weerbaarheid van gemeente Den Haag. We zorgen er daarbij waar mogelijk voor dat de betrokken personen beschikken over het mandaat dat zij nodig hebben om - gevraagd en ongevraagd - wijzigingen door te voeren.

Wanneer we het hebben over een correcte inzet van mensen, dan kunnen we vorm en inhoud van communicatie ook niet onvermeld laten. Het is namelijk niet voldoende wanneer uw ICT-afdeling alleen melding maakt van een technische kwetsbaarheid, zonder deze te vertalen naar het risico dat deze vormt voor een bepaalde afdeling of systeem. Ook de kans op het risico is een bepalende factor voor de te ondernemen activiteiten. Communicatie vanuit ICT staat of valt met de mate waarin deze is aangepast aan de kennis van de doelgroep waarvoor deze is bestemd en het kanaal dat wordt gebruikt om de boodschap over te brengen. Betrek iedereen bij wat u doet; ICT én mensen uit de organisatie. Deze laatsten moeten namelijk concreet aan de slag met het oplossen van de kwetsbaarheden. Hoe sneller zij stappen ondernemen, hoe minder ze hoeven op te lossen. Binnen onze gemeente besteden we daarom veel aandacht aan het informeren van alle betrokkenen. Door de positieve effecten van de inspanningen inzichtelijk te maken, verwachten wij iedereen uiteindelijk zover te krijgen dat ze zelf mee gaan denken en risico's aanpakken voor het problemen worden.

Een goed functionerende ICT-afdeling heeft duidelijke **processen** met aandacht voor zaken als asset management, patch management, change management en vulnerability management. Deze worden in hoofdstuk 2.2 besproken.

Zodra de elementen 'mensen' en 'processen' naar behoren zijn uitgewerkt en ingevuld, kunt u zoals eerder aangegeven, gaan kijken welke **technologieën** het beste aansluiten bij de behoefte. In het onderdeel 'ondersteunende technologie' in hoofdstuk 2.3 gaan we uitgebreider in op:

- software die helpt om de digitale voetprint en het aanvalsoppervlak van uw organisatie inzichtelijk te maken,
- systemen die helpen bij het coördineren van en inzicht in diverse activiteiten en
- bug bounty platformen waarmee u uw samenwerking met hackers vorm kunt geven.

Teamwerk

Binnen het expertisecentrum security van gemeente Den Haag is sprake van een grote mate van onderlinge samenwerking, gebaseerd op onderling vertrouwen. Peter van Eijk, Information Security Manager bij gemeente Den Haag: "Binnen het team is er ook voldoende strijd, maar altijd over de inhoud. Je hoeft het niet altijd met elkaar eens te zijn, op basis van een goede discussie ontstaat het meest uitgebalanceerde advies en het beste resultaat. Zonder wrijving geen glans tenslotte, waarbij je natuurlijk ook weer niet te lang door moet wrijven want dan slaat de vlam in de pan. De onderlinge samenwerking is gebaseerd op vertrouwen; we leveren conform afspraak en geven op sterke argumenten gebaseerd advies waarmee de business een goede afweging kan maken welke actie zij nodig acht.

Vragen om te bepalen of uw ICT-afdeling klaar is voor structurele verbeteringen op het gebied van digitale veiligheid

- Van welk percentage assets is de verantwoordelijke onbekend?
- Heb ik op elk moment inzicht in het aanvalsoppervlak van onze organisatie?
- Zien wij cyberaanvallen aankomen?
- Hoe vaak testen wij onze systemen op dataveiligheid?
- Zijn wij in staat om de uitkomsten van deze testen adequaat te prioriteren en op te volgen?

> Mensen, processen en technologie bepalen de mate waarin een ICT-afdeling haar basis op orde heeft.

Vertegenwoordigers van de security- en ICT-afdeling van gemeente Den Haag zijn 24 uur per dag, 7 dagen in de week beschikbaar. Er is altijd een specialist beschikbaar om in te springen als het nodig is. Als onze CISO belt omdat hij een nieuwe ontwikkeling of dreiging in de buitenwereld voorbij heeft zien komen, zijn

wij er meestal al mee aan de slag. Door de voorkant van het proces goed in te richten, zijn we in staat potentieel gevaar tijdig te signaleren, goed in te schalen en passende maatregelen te nemen die voorkomen dat het uit de hand loopt. Voor de medewerkers en verantwoordelijken van de betrokken afdelingen lopen werk en privé vaak door elkaar vanwege de persoonlijke interesse in het vakgebied. Zij duiken overal in en gebruiken elke vrije minuut om via online fora, evenementen, webinars en andere informatiebronnen op de hoogte te blijven van de laatste ontwikkelingen. Digitale beveiliging gaat zeker niet alleen om techniek, ook dit is en blijft mensenwerk.

Het is de kunst om klein te beginnen en stap voor stap toe te werken naar de stip op de horizon. Per use case bepalen wat ervoor nodig is om deze te realiseren en hoe dit kan worden geregeld, leidt op termijn tot een organisatie die op een professionele manier met hacks om kan gaan.

Het expertisecentrum security bedient zowel de ICT-afdeling als de rest van de organisatie. Op die manier vergroten we de impact op de werkzaamheden die binnen de gemeente worden uitgevoerd, geven we eenduidig richting aan activiteiten en kanaliseren we communicatie en activiteiten op een adequate manier. Ook samen sparren is op deze manier eenvoudiger. Een cyberaanval op gemeente Den Haag is tegenwoordig niet meer alleen een veiligheids- en ICT-issue, maar een aanval op het hele gemeentelijke Expertise Team Security, ICT én de business.”

2.2 INRICHTEN PROCESSEN

Er is sprake van een continue wisselwerking tussen processen en tools die worden ingezet in het kader van digitale weerbaarheid. De tools geven ons inzichten op basis waarvan we onze processen optimaliseren. Zien we bijvoorbeeld dat bepaalde kwetsbaarheden op verschillende plekken voorkomen, dan kunnen we succesvolle oplossingen ook op andere plekken inzetten. Komen bepaalde gebreken herhaaldelijk terug, dan passen we daar onze aansluitingsvoorwaarden op aan. Telkens wanneer we een stap verder maken in het verfijnen van onze processen, komen hier automatisch weer nieuwe eisen en wensen voor de tools uit naar voren. Ook bij het inrichten van processen geldt dat u ergens zult moeten beginnen. Onderstaand is een aantal belangrijke processen beschreven, waarmee u de basis legt voor de uitvoering van uw beleid en strategie voor digitale veiligheid.

Asset management

Met ICT-asset management beheert u de inventaris en levenscyclus van de ICT-middelen waar uw organisatie over beschikt. Hardware, software en de bijbehorende licenties moeten voortdurend worden onderhouden, bijgewerkt,

gerepareerd en vervangen. Goed asset management zorgt voor inzicht in de ICT-middelen die een organisatie bezit en een proces om deze gegevens actueel te houden. Als dit proces goed is ingericht, heeft u inzicht in alle assets die bij uw organisatie horen en is duidelijk onder wiens verantwoordelijkheid ze vallen. Beide zijn nodig voor het continu doorvoeren van verbeteringen in het kader van digitale veiligheid. Asset management kan worden belegd bij de eigen organisatie of worden uitbesteed aan een derde partij.

Patch management

Het volgende proces dat een cruciale rol speelt bij digitale veiligheid betreft patchen. Een patch is een installatiebestand dat een kwetsbaarheid of fout in een programma herstelt of een programma verbetert door bijvoorbeeld extra functionaliteit toe te voegen. Kwetsbaarheden in een programma of een website vormen een potentiële bedreiging voor de informatieveiligheid van een organisatie. Daarom dient elk bedrijf een goed plan van aanpak te hebben om gevonden kwetsbaarheden zo snel mogelijk te verhelpen. Patchen is vaak een complex proces omdat één wijziging meerdere systemen kan raken. Het is de kunst om fouten op de gewenste plek te repareren, zonder dat daarbij (onbedoeld) op andere plaatsen nieuwe problemen ontstaan. Patches worden daarom uitgebreid getest voordat ze worden doorgevoerd. Dat kan zowel handmatig als geautomatiseerd. Alleen met een strak ingericht patch management proces waarmee u 24 uur per dag, 7 dagen in de week patches door kunt voeren, kan er sprake zijn van een succesvolle uitvoering van het beleid voor digitale veiligheid.

Change management

Het derde proces dat een belangrijke rol speelt bij digitale veiligheid is het proces om veranderingen door te voeren. Change management wordt gedefinieerd als methodes en manieren waarop organisaties veranderingen doorvoeren in interne en externe processen. Dit gaat over het voorbereiden en ondersteunen van medewerkers, bepalen van de nodige stappen waarin de wijziging wordt doorgevoerd en het controleren van activiteiten vóór en na doorvoering om er zeker van te zijn dat de aanpassing correct is gedaan. Grote en kleine veranderingen in ICT-systemen kunnen voor problemen zorgen omdat ze impact hebben op allerlei onderdelen, systemen en personen binnen een organisatie. Goede communicatie over de door te voeren aanpassing is daarom een van de belangrijkste succesfactoren van effectief change management. Basis op orde in de ICT-afdeling betekent dus ook dat er sprake is van een gestructureerde aanpak voor het doorvoeren van veranderingen.

Bij gemeente Den Haag verloopt elke aanpassing van ICT-componenten structureel via de change management keten om er zeker van te zijn dat we geen en-

kel element dat door de verandering wordt geraakt, over het hoofd zien. Noodzakelijke wijzigingen zijn 9 van de 10 keer dienstoverstijgend. Een zorgvuldige, gecontroleerde en veilige wijze van doorvoeren van wijzigingen bestaat daarom voor een groot deel uit intensief overleg met betrokken partijen. Welke ingrepen zijn precies nodig, wat is het risico van deze acties, hoe lang zijn betreffende systemen niet beschikbaar voor de dienstverlening? De doorlooptijd van de aanpassing en het soort dienstverlening dat wordt getroffen, bepalen het juiste moment voor de uit te voeren actie. Het kassasysteem van de gemeentezwembaden gaan we niet patchen midden op een zomerse dag wanneer de halve gemeente naar binnen wil.

Vulnerability management

Het vierde proces gaat over vulnerability management. Dit zijn activiteiten die een organisatie onderneemt om er voortdurend voor te zorgen dat zwakke plekken in de eigen digitale systemen worden opgespoord en hersteld. Een proces waarbij mogelijke kwetsbaarheden van digitale assets proactief worden geïdentificeerd, geanalyseerd, ingeschaald en opgelost. Hierbij wordt de totale levenscyclus van de kwetsbaarheden van A tot Z bijgehouden zodat geen enkel potentieel risico tussen de wal en het schip belandt. Hoe complex een dergelijke omgeving ook is. Vulnerability management gaat over risicoacceptatie en -mitigatie. Als de security- en ICT-afdeling tot de conclusie komen dat er sprake is van een kwetsbaarheid met een negatieve impact op de organisatie, dan kunnen zij maatregelen nemen om het risico te minimaliseren. Maar de eigenaar van de getroffen systemen heeft uiteindelijk de verantwoordelijkheid en bepaalt wat er met het risico én het advies gebeurt.

Ondanks recente berichtgeving over grote hacks en kostbare gevolgen, treffen veel organisaties nog steeds slechts minimale maatregelen als het gaat om digitale veiligheid. Maar met standaard patch management en wat antivirussoftware

TIPS

- Maak voor security-gerelateerde wijzigingen gebruik van de standaard change management processen. Dit zorgt ervoor dat de processen veel beter bij de betrokkenen beklijven. De doorlooptijd van wijzigingen op het gebied van veiligheid is het enige dat afwijkt van de standaard.
- Zorg voor duidelijke afspraken met, begeleiding van en informatievoorziening voor de supportafdeling zodat zij een goede inschatting maken of iets een security incident is of niet. Alleen het feit dat een medewerker een phishing e-mail ontvangt is geen security incident; dat wordt het wel zodra er op de link is geklikt.
- Kies bij security-gerelateerde wijzigingen met een hoge prioriteit voor een warme overdracht aan de ICT-afdeling. Daarmee is het belang van snelheid eerder duidelijk en vergroot u de kans dat de ICT-collega's standaard werkzaamheden laten liggen en hun tijd en aandacht besteden aan het zo snel mogelijk oplossen van het security-incident.
- Laat ICT-medewerkers bij twijfel altijd direct schakelen met collega's van de afdeling security.

creëert u geen verdediging waar een gemiddelde crimineel voor terugdeinst. Door het continu uitvoeren van vulnerability scans blijft u geïnformeerd over het veranderende dreigingslandschap en komen kwetsbaarheden aan het licht die in de dagelijkse praktijk onopgemerkt blijven. Uit de opgebouwde historie komen ontwikkelingen en trends naar voren die bepalen of de door u ingestelde maatregelen voor de digitale veiligheid nog steeds effectief zijn op het gebied van mens, proces en technologie.

Security en ICT schalen een kwetsbaarheid als negatief en impactvol in en adviseren maatregelen om het risico te minimaliseren. Maar de eigenaar van de getroffen systemen is uiteindelijk verantwoordelijk en bepaalt wat er met het risico én het advies gebeurt.

Gaat u nog een stap verder dan kunt u penetration tests (pen-testen) laten uitvoeren waarbij u gespecialiseerde hackers inzet die de kwetsbaarheden die zij vinden, daadwerkelijk gebruiken om in systemen in te breken en te kijken hoever ze kunnen komen. Deze testen leveren interessante inzichten op hoe moeilijk of makkelijk het uiteindelijk voor specialisten is om in uw systemen in te breken en hoe snel gevoelige gegevens dan op straat liggen. In het volgende hoofdstuk gaan we in op verschillende vormen van technologische ondersteuning die concreet bijdraagt aan het verbeteren van de digitale veiligheid van uw organisatie.

2.3 ONDERSTEUNENDE TECHNOLOGIE

Denk groot, maar begin klein. Ga niet gelijk alles aanzetten voor elke optie die bestaat. Start met een beperkte scope: hoe lopen interne processen, zijn alle assets geregistreerd. Kijk wat werkt en wat niet en breid dit langzaam uit.

Door bij uw keuze voor ondersteunende technologie in te zetten op strategische partnerships met de betreffende leveranciers, beschikt u over meer kennis en ervaring om het belang van digitale veiligheid en weerbaarheid binnen uw organisatie goed op de kaart te zetten.

Technologie speelt een steeds grotere rol in ons dagelijkse leven. Ook bij het realiseren van goede digitale beveiliging. Waaruit deze ondersteuning bestaat? Uit applicaties die inzichtelijk maken over welke informatie, websites en systemen u beschikt én wie hiervoor uiteindelijk verantwoordelijk is. Systemen waar u relevante gegevens in vast kunt leggen en ontwikkelingen kunt volgen zodat u beschikbare tijd, geld en capaciteit zo efficiënt mogelijk in kunt zetten. En tenslotte zijn er de platformen om met hackers samen te werken en hun kennis en kunde in te zetten om kwetsbaarheden te achterhalen vóórdat criminelen hier misbruik van maken.

Digitale voetprint en aanvalsoppervlak

Toen gemeente Den Haag in 2007 serieus aan de slag ging met digitale veiligheid, bleek dat er beperkt zicht was op de digitale voetprint en het aanvalsoppervlak van de organisatie. Een digitale voetprint verwijst naar alle sporen die een

persoon achterlaat tijdens het gebruik van internet. Informatie die online wordt verzonden, zoals bijvoorbeeld ingevulde formulieren, verstuurde e-mails en bijlagen, het uploaden van video's of digitale afbeeldingen en elke andere vorm van overdracht van informatie. Sporen van persoonlijke informatie over wie u bent en wat u doet wordt daarmee online beschikbaar voor anderen.

Het aanvalsoppervlak van een organisatie bestaat uit diverse assets zoals websites, domeinen, servers en hostdiensten die op verschillende manieren kunnen worden aangevallen waarbij de indringer gegevens kan onderscheppen. Door het aanvalsoppervlak van uw organisatie te analyseren en te beheersen, kunt u het risico van cyberdreigingen terugdringen. Iets waar zowel grote als kleine organisaties actief mee bezig zouden moeten zijn. Want als onduidelijk is over welke systemen en websites en dergelijke uw organisatie beschikt, kunt u deze niet beschermen en is onduidelijk wat de gevolgen van een aanval zouden zijn.

Het analyseren en beheren van de digitale voetprint en het aanvalsoppervlak kan in eigen beheer worden uitgevoerd of worden uitbesteed aan een specialist. Met behulp van speciaal voor dit doel ontwikkelde platformen, worden de assets van uw organisatie op een rij gezet en vervolgens gemonitord. Bij gemeente Den Haag hebben we gekozen voor het Attack Surface Management platform van Cybersprint. Belangrijke elementen die meespeelden bij deze keuze waren de brede inzetbaarheid en schaalbaarheid van het platform en de afspraken die we met de leverancier konden maken over de door ons gewenste servicelevels.

Factoren bij selectie van een ASM platform

- Automatisering (schaalbaarheid)
- Integratie in processen
- Gepersonaliseerde rapportage

Gemiddeld komen er via dit soort platformen 30-35% meer assets boven tafel dan organisaties van tevoren zelf op de radar hebben. En elke asset kent weer haar eigen kwetsbaarheden. Het in kaart brengen van het speelveld en bijbehorende risico's is één ding, maar deze goed opvolgen, is weer iets heel anders. Daarom is het cruciaal dat interne processen hier goed bij aansluiten en dat er sprake is van borging binnen de organisatie. Een van de dingen waar wij bij de gemeente tegenaan liepen, was het achterhalen van de eigenaar van de assets, de verantwoordelijke voor het oplossen van de gevonden kwetsbaarheden. En is de eigenaar eenmaal gevonden, dan is het nog een uitdaging om deze mensen te overtuigen van de noodzaak om actie te ondernemen. Of om intern urgentie te krijgen om een aanpassing met spoed door het proces te krijgen.

Omdat we bij de gemeente steeds meer software naar de cloud brengen, vinden we het belangrijk om te weten welke security risico's en kwetsbaarheden we in

onze supply chain lopen. Het Cybersprintplatform helpt ons hier snel inzicht in te krijgen, waarna we effectief de dialoog aangaan met derde partijen over hun veiligheidsmaatregelen. Ook vormt het platform een belangrijke schakel in het opsporen van shadow-IT en malicious websites. Dit laatste helpt ons om in een vroegtijdig stadium eventuele phishing aanvallen te signaleren en risicoverlagende maatregelen te treffen.

Als gemeente Den Haag hebben we er bewust voor gekozen het inventariseren van onze digitale voetprint en het in kaart brengen en monitoren van ons aanvalsoppervlak gedoseerd te doen. Stap voor stap hebben we steeds meer modules ingezet en de dienstverlening uitgebreid. Van het Attack Surface Management platform naar de Social Media module en de Managementmodule. De volgende stap is het inzetten van de DMARC Monitor om onze e-mailstromen beter te beveiligen en het nog beter inzetten van het platform om makkelijker te voldoen aan de eisen die worden gesteld in de Baseline Informatiebeveiliging Overheid (BIO). De tools waarmee we werken, helpen ons daadwerkelijk bij het behalen van de doelstelling 'benutting van technische kwetsbaarheden voorkomen'.

Naast de kwetsbaarheiden die je met eigen inspanningen signaleert, zijn er tal van instanties die informatie hebben over hacks die wereldwijd bekend zijn. Organisaties als het IBD, NCSC en hacker websites houden continue in de gaten wat er speelt en geven advies hoe je om kunt gaan met bevindingen. De ervaring leert echter dat je niet standaard uit moet gaan van de aanbevelingen van derden zonder goed na te denken over specifieke gevolgen voor je eigen organisatie. Het kan namelijk zo maar zijn dat er al andere maatregelen zijn genomen waardoor een risico al voldoende wordt afgezwakt.

Het aanschaffen van instrumenten voor het monitoren van uw digitale voetprint en het aanvalsoppervlak is een eerste stap. Het succesvol opvolgen van de aanbevelingen voor het verlagen van de risico's, bepaalt uiteindelijk de meerwaarde die u daarmee voor de organisatie creëert. Applicaties die helpen bij het inplannen en volgen van de nodige activiteiten dragen hier aanzienlijk aan bij, omdat ze het werk efficiënt te laten verlopen en helpen om overzicht te houden. De belangrijkste coördinerende systemen komen hierna aan bod.

> Het binnenhalen van een goede tool is stap 1. Het succesvol opvolgen van de aanbevelingen voor het verlagen van de risico's bepaalt uiteindelijk de meerwaarde voor de organisatie.

Coördinerende systemen

Het adequaat opvolgen van geïdentificeerde kwetsbaarheden is een kwestie van keuzes maken en waar mogelijk gebruikmaken van ondersteunende techniek. Beide zijn even belangrijk. Voor wat betreft keuzes maken, geldt het volgende.

Met beschikbare technologie kunt u de hele wereld scannen, maar dan komt er zóveel informatie terug dat het al snel niet meer te behappen is. Beperk uw scope, richt u in eerste instantie op wat nodig is om de kroonjuwelen van uw organisatie goed te beschermen. Focus op dingen die echt pijn doen en eenvoudig op te lossen problemen. Houd daarbij voor ogen dat het onmogelijk is om alles tegelijkertijd op te lossen. Zolang u bekend bent met de risico's en een goede afweging kunt maken of u iets nu of later aanpakt, dan bent u in control. Het tweede punt, gebruikmaken van ondersteunende techniek, gaat over het steeds verder automatiseren van uit te voeren activiteiten, menselijk handelen. Werkt u hierbij volgens een vast proces zoals bijvoorbeeld de 'Plan, Do, Check en Act cyclus', dan minimaliseert u de kans op het maken van fouten en voorkomt u dat cruciale stappen over het hoofd worden gezien.

Overwegingen bij evaluatie van coördinerende tools

- Bestaat de mogelijkheid om backlog op te nemen?
- Kunnen we use stories eenvoudig bij het juiste disciplinaire team beleggen?
- Is er sprake van enkelvoudig of meervoudig gebruik van data?
- Wat zijn minimale eisen aan rapportage?

Coördinerende systemen helpen om de administratieve overhead te beperken. Rapportage staat hierbij centraal, liefst in de vorm van dashboards zodat sturing van de organisatie berust op goed onderbouwde argumenten. Gemeente Den Haag wil meer datagestuurd en informatiegedreven werken en op basis daarvan hebben we diverse tools geselecteerd. Het blijft echter niet bij een eenmalige evaluatie en selectie, we blijven constant toetsen of systemen nog steeds bijdragen aan de gestelde doelen of dat we verzanden in een administratieve exercitie.

Er is altijd sprake van een spanningsveld tussen agile werken en processen. Agile gaat over zelf organiseren, eigen initiatief. Maar in hoeverre mag een ISO of een ICT-medewerker een wijziging doorvoeren zonder dat de impact hiervan door anderen is onderzocht? De juiste coördinerende tools dragen bij aan afstemming van acties over afdelingen heen.

Configuration Management Database (CMDB)

De assets die u met het in kaart brengen van het aanvalsoppervlak van uw organisatie boven tafel heeft gekregen, wilt u op een gestructureerde manier onderbrengen in een database samen met de bijbehorende risicoclassificatie. Deze data kunt u vastleggen in een Configuration Management Database. Door structurele vastlegging zorgt u ervoor dat de informatie actueel blijft en dat de verschillende assets effectief worden gemanaged. Omdat de hoeveelheid ge-

vonden assets en (potentiële) kwetsbaarheden vaak groter is dan de beschikbare capaciteit om deze op te lossen, kunt u ervoor kiezen de assets die niet binnen uw eigen domeinen vallen tijdelijk 'te parkeren'. Bij het behandelen van de assets, volgt u de prioritering en het handelingsperspectief (wat zijn mogelijke oplossingsrichtingen voor de gevonden issues) die u worden aangeboden door het platform dat uw aanvalsoppervlak en digitale voetprint in de gaten houdt. Prioriteit ligt bij kwetsbaarheden van systemen die bij uitval direct impact hebben op de continuïteit van uw dienstverlening.

Als gemeente Den Haag hebben we ook laaghangend fruit direct meegenomen: eenvoudig op te lossen issues die laten zien dat het investeren in digitale veiligheid de moeite waard is en dat hiermee veel problemen worden voorkomen.

ICT Service Management Systeem (ITSM)

ICT Service Management staat voor het procesmatig aansturen van de werkzaamheden die horen bij het ICT-beheer van een organisatie. Het ICT Service Management Systeem is gebaseerd op ITIL-processen wat staat voor Information Technology Infrastructure Library. In deze bibliotheek staan de beste praktijkoplossingen beschreven op het gebied van beheer van Informatie Communicatie Technologie. Met andere woorden: richtlijnen die aangeven hoe een ICT-dienstverlener of -afdeling kan waarborgen dat haar klanten de producten en diensten krijgen die zij verlangen. Met behulp van een ITMS en genoemde ITIL-processen worden aanpassingen in de ICT-infrastructuur op een gestructureerde en gecoördineerde manier doorgevoerd. Vooraf wordt een uitgebreide impactanalyse gedaan en gezorgd voor goede back-ups zodat het mogelijk is om terug te gaan naar het moment vóór een probleem ontstond of voordat een wijziging werd doorgevoerd.

Weet u zeker dat back-ups binnen uw organisatie correct worden uitgevoerd? Zet zo nu en dan de complete back-up van systemen eens terug en toets of deze mogelijk aan consistentie en volledigheid te wensen overlaat.

ITSM is software die ICT-afdelingen helpt bij het beheren en beheersen van deze processen. Het ITMS ondersteunt bij:

- Configuratiebeheer / ICT asset management waarmee alle relevante informatie over uw configuraties en de afzonderlijke ICT-middelen wordt gedocumenteerd en bijgehouden.
- Incidentenbeheer, één van de belangrijkste onderdelen van uw ICT-afdeling omdat dit ervoor zorgt dat u klantvriendelijk en snel kunt reageren op incidenten.

- Probleembeheer waarbij vaak voorkomende incidenten met behulp van de software worden geïdentificeerd en noodzakelijke vervolgstappen worden ondernomen om gelijksoortige toekomstige incidenten te voorkomen.
- Wijzigingsbeheer waarmee u bijhoudt welke veranderingen en aanpassingen u doorvoert in uw ICT-omgeving.

In het ICT Service Management Systeem van gemeente Den Haag worden gewenste acties voor het oplossen van gevonden kwetsbaarheden inmiddels automatisch omgezet naar werkbriefjes voor collega's die ermee aan de slag gaan. Afmelding wordt in hetzelfde systeem gedaan, waarna er controle plaatsvindt om te kijken of de opvolging effectief is geweest. Nieuwe inzichten die op deze manier ontstaan, gebruiken we om bestaande processen steeds verder te optimaliseren.

Coördinerende applicaties zijn als standaard producten beschikbaar in de markt. Welke het beste passen binnen uw organisatie is afhankelijk van de missie die u uzelf heeft gesteld, de eisen waaraan de functionaliteit moet voldoen en integratie met reeds aanwezige oplossingen binnen uw organisatie. Het goed inrichten van interne processen is bepalend voor de bijdrage die systemen leveren. Dus bedenk van tevoren wie binnen de organisatie verantwoordelijk is voor het oppakken, beoordelen en doorzetten van gemelde kwetsbaarheden.

Bug bounty platformen

Steeds meer organisaties en softwareontwikkelaars introduceren een eigen bug bounty programma om op die manier de kennis van hackers in te zetten om kwetsbaarheden op te sporen in online applicaties en websites. Voordat u een bug bounty programma introduceert, geeft u met een Coordinated Vulnerability Disclosure op uw website aan dat uw organisatie hackers de mogelijkheid geeft om gevonden kwetsbaarheden te delen, zonder dat dit juridische of strafrechtelijke consequenties heeft. De Coordinated Vulnerability Disclosure en bug bounty programma's worden in hoofdstuk 2.4 (betrekken van een hacker community) in meer detail behandeld.

Om het bug bounty-programma van gemeente Den Haag goed te managen, hebben we ervoor gekozen om te werken met het platform van Zerocopter. Hier melden hackers gevonden kwetsbaarheden. Naast de functionaliteit van het platform was ook in dit geval de bereidheid van de leverancier om een proactieve bijdrage te leveren aan de digitale weerbaarheid van gemeente Den Haag een bepalende factor. Daarnaast heeft Zerocopter een goede relatie met een grote hacker community, een cruciale factor voor het uiteindelijke succes van het

programma. Andere voordelen zijn dat de hackers die via het platform werken, van tevoren zijn gescreend en dat vermeende kwetsbaarheden goed worden gerapporteerd.

De communicatie met de hackers verloopt ook via het platform en niet via e-mail. Hiermee voorkomen we dat derden geïdentificeerde kwetsbaarheden onderscheppen en misbruiken. Wij hebben er bovendien voor gekozen om de specialisten van Zerocopter een eerste triage van gemelde kwetsbaarheden voor ons te laten doen. Op die manier zette we onze eigen mensen optimaal in voor het interpreteren van de mogelijke impact op de beschikbaarheid van onze systemen en voor de afstemming met de getroffen diensten. Vanuit het oogpunt van kostenefficiëntie doet Zerocopter ook de financiële afhandeling van het programma, wat zij sneller en met minder moeite realiseren dan wanneer we dit als gemeente zelf zouden doen.

BUG BOUNTY PLATFORM IN ACTIE

Zerocopter levert het platform dat gemeente Den Haag inzet voor de uitvoering van haar bug bounty programma en dat eveneens wordt gebruikt om de tijdens Hâck The Hague gevonden hacks in te registreren. Chantal Stekelenburg, Head of Operations en Edwin van Andel, CEO bij het bedrijf vertellen hoe dit soort platformen in de praktijk het verschil maken.

Edwin: "Het Zerocopter platform wordt dagelijks door onszelf ingezet om de communicatie met hackers die voor ons bij opdrachtgevers werken, te faciliteren. In het platform kunnen zij bijvoorbeeld de briefing van de klant vinden voor ze beginnen aan de opdracht. Ook wordt het platform gebruikt als bug bounty administratie, dus om hacks vast te leggen en te bepalen voor welke compensatie hackers in aanmerking komen. Het is ook het platform waarmee we templates voor Coordinated Vulnerability Disclosures ter beschikking stellen aan bedrijven".

"Tijdens Hâck The Hague wordt het platform gebruikt om gevonden kwetsbaarheden te registreren", gaat Chantal verder. "Aan de 'andere kant van het systeem' zit ik samen met vertegenwoordigers van de Gemeente Den Haag om alle hacks die binnenkomen te bekijken. Gaat het om een echte kwetsbaarheid of is het een duplicaat? Hoe groot is de impact? Is het aangeleverde rapport over de hack volledig en duidelijk? Vervolgens bepalen we welke hacks naar ons idee in aanmerking komen voor een prijs en waarom. Uiteindelijk bepaalt de jury wie de echte winnaars zijn. Bijkomend voordeel van het platform is dat er een tijdcode aan de gelogde hacks wordt toegevoegd. Dat komt goed van pas voor het geval identieke hacks vlak na elkaar worden gelogd. Dan ben je blij dat je op de seconde kunt kijken wie er eerder was."

Edwin: "Ontwikkelingen aan bug bounty-platformen staan niet stil. Sommige nieuwe functionaliteit maakt het leven van hackers makkelijker, bijvoorbeeld door een uitbreiding van categorieën waaruit hackers kunnen kiezen om een passend label te vinden voor de door hen gevonden kwetsbaarheid. Andere dingen helpen bij de organisatorische kant van het bug bounty programma; bijvoorbeeld de common vulnerability scoring system calculator die met behulp van bepaalde formules helpt bepalen hoe groot de impact van een gevonden hack is. Zijn er bijvoorbeeld heel veel stappen nodig vóór je bij de gevonden kwetsbaarheid komt, dan wordt de kans kleiner dat dit daadwerkelijk gebeurt en is de impact dus lager. Ook als er interactie met een gebruiker van het systeem nodig is om een hack te laten slagen (het laten klikken op een link bijvoorbeeld) neemt de waarschijnlijkheid dat de hack ooit voor zal komen af. Dat zijn allemaal elementen waar deze nieuwe calculator rekening mee houdt.

Maar het grootste verschil wordt gemaakt door de hackers die met het bug bounty platform werken. Door een bug bounty platform in te zetten, krijgt uw organisatie toegang tot de kennis en kunde van gescreende experts van over de hele wereld en krijgt u na het definiëren van een specifiek project, goedgeschreven en gevalideerde rapporten eenvoudig via uw eigen dashboard aangeleverd."

2.4 BETREKKEN VAN EEN HACKER COMMUNITY

De ontwikkelingen in ICT gaan razendsnel en hetzelfde geldt voor de tools en technieken die criminelen inzetten om systemen te breken en te misbruiken in hun eigen voordeel. Het hoge tempo waarin veranderingen plaatsvinden en innovaties het licht zien, maakt het bijna onmogelijk om zonder hulp van externe specialisten optimaal gebruik te maken van de mogelijkheden die de technologie biedt. Waar het digitale veiligheid aangaat, zijn hackers de experts. Zogenaamde ethische (eerlijke) hackers zijn personen die op zoek gaan naar kwetsbaarheden van soft- en hardware zoals websites, computersystemen en netwerken en deze kwetsbaarheden niet openbaar maken, maar de betreffende organisaties informeren over het lek om hen de kans te geven hun zaken op orde te krijgen.

Ondanks het feit dat hackers nog steeds door veel organisaties met argusogen worden bekeken, hebben zij al menig rampscenario voorkomen. Ze helpen bedrijven en overheidsinstellingen veiligheidsrisico's in kaart te brengen en doelgericht de ICT-beveiliging verbeteren. Gaat u samenwerken met hackers, zorg er dan voor dat u deze community serieus neemt. Vindt een hacker zelf of op verzoek een kwetsbaarheid in uw systemen, reageer dan snel en communiceer transparant. Houd de melder op de hoogte van de voortgang tot de kwetsbaarheid is opgelost. Blijf qua beloning niet hangen in de fase van leuke T-shirts of een mok, maar zorg ervoor dat de beloning en de credits die een hacker krijgt voor het melden van een kwetsbaarheid in verhouding staan met de problemen die met deze ontdekking worden voorkomen.

Om een goede relatie op te bouwen met de hacker community is het goed om leveranciers en partners uit te zoeken die zelf goed bekend staan in de hackerwereld en beschikken over een goed netwerk binnen deze doelgroep. Met onderstaande onderwerpen kunt u uw samenwerking met hackers stap voor stap professionaliseren.

Coordinated Vulnerability Disclosure (CVD)

Het doel van een Coordinated Vulnerability Disclosure (voorheen Responsible Disclosure) is om bij te dragen aan de veiligheid van ICT-systemen door kennis over kwetsbaarheden te delen zodat anderen hier hun voordeel mee kunnen doen. Door een CVD-policy op te nemen op de website, geeft een organisatie hackers de mogelijkheid om gevonden kwetsbaarheden met hen te delen zonder dat dit voor de hacker nadelige gevolgen heeft. In de CVD-policy zijn regels opgenomen voor zowel de hackers als de organisatie zelf. De hackers stemmen in met het op een gecoördineerde wijze bekend maken van een kwetsbaarheid nádat deze is opgelost. De organisatie klaagt de hacker niet aan voor inbreuk op haar systemen en houdt de melder van de kwetsbaarheid op de hoogte van de

vorderingen bij het oplossen ervan. Er zijn verschillende informatieve websites die een eerste opzet voor een CVD aanbieden welke u naar eigen inzicht aan kunt passen.

Bug bounty programma

Met het opzetten van een bug bounty programma gaat u nog een stapje verder dan bij de CVD. U kent dan ook een beloning toe aan kwetsbaarheden die een hacker via de CVD bij u meldt. Een bug bounty programma is dus eigenlijk een beloningsprogramma voor het opsporen van kwetsbaarheden in de ICT-systemen en infrastructuur van een organisatie. Het is een mooie aanvulling op reguliere tests en controles op bestaande beveiligingsmaatregelen omdat u hiermee een groter aantal personen aantrek die uw systemen blijven testen. Beschikt uw organisatie over een grote hoeveelheid aan gevoelige data en/of zijn de gevolgen van een criminele hack potentieel groot? Dan is het zeker de moeite waard om een bug bounty programma in te zetten. Via dergelijke programma's profiteert u namelijk van de inzet van een groot netwerk van hackers wiens kennis en kunde ervoor zorgen dat u dataverlies en reputatieschade kunt voorkomen.

Beschikt uw organisatie over een grote hoeveelheid aan gevoelige data en/of zijn de gevolgen van een criminele hack potentieel groot? Dan is het zeker de moeite waard om een bug bounty programma in te zetten.

Bij gemeente Den Haag hebben wij ervoor gekozen het initiatief om over de kwetsbaarheid te communiceren bij de hacker te leggen. Zodra de gevonden kwetsbaarheid is opgelost en vrijgegeven, mag de hacker hierover communiceren zodat anderen hun voordeel hiermee kunnen doen. Een andere bewuste keuze die wij hebben gemaakt, gaat over het moment van uitbetaling. In de meeste gevallen keren bug bounty programma's alleen uit bij bewezen resultaten, waarmee ze voor organisaties een effectieve manier zijn om hun security budget aan te besteden. Ook bij de gemeente Den Haag werden hackers in eerste instantie uitbetaald op het moment dat de hack was opgelost, waar in specifieke gevallen veel tijd overheen kon gaan. Na verloop van tijd hebben we ervoor gekozen om op het moment dat we een gevonden kwetsbaarheid accepteren tot uitbetaling van de bounty over te gaan. Dit heeft een bijzonder positieve impact gehad op het aantal en de kwaliteit van de kwetsbaarheden dat we krijgen aangeleverd.

Tips

- Het moment van uitbetalen beïnvloedt het aantal en de kwaliteit van gemelde kwetsbaarheden.
- De financiële afhandeling van gemelde hacks kunt u uitbesteden aan het bug bounty platform waarmee u werkt.

Hack-evenement

Veel bedrijven zetten hackathons in om binnen korte, vastgestelde tijd een bepaald probleem op te lossen, een innovatief businessplan te maken of tot nieuwe inzichten te komen. Het hack-evenement waar we het in deze e-guide over hebben, gaat echter over het uitnodigen van hackers om op een vastgesteld moment, binnen vooraf vastgestelde spelregels te kijken welke kwetsbaarheden zij vinden in systemen en websites van de betreffende organisatie en leveranciers die onderdeel uitmaken van hetzelfde ecosysteem. Als een dergelijk evenement goed wordt doordacht, voorbereid én opgevolgd, kan het een perfecte aanvulling zijn op het bestaande programma voor digitale veiligheid. De organisatie vraagt echter ook om een behoorlijke inspanning die niet moet worden onderschat én een strakke regie om te voorkomen dat zaken onbedoeld uit de hand lopen.

Voor uw organisatie overgaat tot het organiseren van een hack-evenement is het goed om na te gaan of

- Uw organisatie qua capaciteit, kennis, processen en tools klaar is om gevonden kwetsbaarheden goed te registreren en op te volgen.

HANDIG OM TE WETEN VOOR HACK-EVENEMENTEN

Welke elementen dragen bij aan het succes van een evenement als Hâck The Hague? Chris van 't Hof is presentator, onderzoeker, schrijven en organisator in informatietechnologie. Hij heeft meerdere publicaties op zijn naam waarin hij de wereld van hackers en security-specialisten van binnenuit beschrijft, waardoor hij deze vraag als geen ander kan beantwoorden.

Chris: "U zou het misschien niet verwachten, maar hackers geven zelf de beste feestjes. Om ook een geslaagd hacker-evenement neer te zetten, is het dus goed om te weten met welke cultuur u te maken heeft. Cultuur staat naar mijn idee voor 'een gedeeld repertoire van gewoontes en symbolische uitingen daarvan'. Bij de hacker community zit het gedeelde repertoire vooral in het zoeken in code en iets vinden waar anderen overheen kijken. Symbolische uitingen uit de hackerscene ziet u bijvoorbeeld terug in het taalgebruik, hoodies en kleurenkeuze bij het aankleden van de locatie om een paar voorbeelden te noemen.

Een ander belangrijke factor die ik hier gelijk wil benoemen, is dat het in deze e-guide niet gaat over het organiseren van hackathons, wat voor veel bedrijven gelijk staat aan een goedkope (zij het vaak intensieve) manier om snel tot innovatieve oplossingen of producten te komen. We hebben het wel over hack-evenementen waarbij een organisatie serieus werk maakt van het verbeteren van de online veiligheid van haar systemen."

Hackers zijn mensen die technologie maken, breken en bespreken

Als iemand die met grote regelmaat hack-evenementen bezoekt en organiseert en in gesprek gaat met leden van de hacker community, denk ik dat onderstaande aspecten van invloed zijn op het al dan niet succesvol zijn van een hack-evenement. De inhoud weegt hierbij zwaarder dan de vorm.

Inhoud

- Doel van het evenement - zorg ervoor dat het echt gaat om het verbeteren van de online veiligheid van systemen en niet de PR. Zo van "Kijk, wij doen ook iets met hackers". Daar zijn hackers echt allergisch voor.
- De scope van de te hacken systemen – Oftewel, hoeveel valt er echt te hacken? Diversiteit en complexiteit moeten voldoende uitdaging bieden. Een extra dimensie wordt toegevoegd wanneer er op de locatie fysieke te hacken objecten staan die

- U een goed overzicht heeft van uw volledige digitale aanvalsoppervlak en het eventuele laaghangend fruit zelf al heeft opgelost of in kaart heeft gebracht.
- Goede en waterdichte spelregels zijn uitgewerkt om het evenement in goede banen te leiden.
- U, zelf of via partners, de bij het evenement te betrekken hackers in beeld heeft en deze kunt benaderen.
- U beschikt over de capaciteit om de interne en externe communicatie rond het evenement adequaat vorm te geven, qua inhoud en wat betreft de in te zetten kanalen.
- De technische infrastructuur beschikbaar is om het evenement goed te laten verlopen en te monitoren.

En tenslotte wilt u ervoor zorgen dat u de juiste mensen bij het evenement betrekt. Want het organiseren van een hack-evenement lijkt misschien voornamelijk om techniek te gaan, maar uiteindelijk valt en staat het met de inzet van de juiste mensen. Enthousiaste, gemotiveerde, betrokken personen die een aan-

tot de verbeelding spreken.

- Goede opvolging - Wordt er serieus iets gedaan met de gevonden kwetsbaarheden en worden de vinders hiervan op de hoogte gehouden? Sommige kwetsbaarheden zijn snel op te lossen. Meld dat. Maar het kan ook zijn dat iets voorlopig niet te fixen is. Dan moet u wel met goede argumenten komen waarom dat zo is.
- Groepsdynamiek - Wie komt er nog meer? Een hack-evenement is bij uitstek een mogelijkheid voor hackers om anderen te ontmoeten die ze alleen van online kennen of personen met een relevante reputatie.
- Kwaliteit van de jury - De personen die uiteindelijk jouw hacks behoordelen, moeten wel mensen zijn die het snappen (geloofwaardigheid). Zijn het bekenden uit de scene, dan trekken ze ook weer veel goede deelnemers aan.

Vorm

- Zorg voor een prettige, toegankelijke locatie. Hackers willen gewoon hacken en niet teveel gedoe eromheen. Mogelijkheden van de locatie zijn belangrijker dan de status.
- Onmisbare elementen voor wat betreft de catering voor een hack-evenement zijn Club-Mate (een cafeïne- en koolzuurhoudende frisdrank), snacks, red bull en pizza (maar géén alcohol!)
- Hackers zijn gek op swag - het modieuze acroniem voor 'Stuff We All Get', oftewel allerhande relatiegeschenken als hoodies, apparaatjes, stickers, keycords en dergelijke.

Tot slot

De hackerscene bestaat helaas voornamelijk uit mannen. Koester die enkele vrouwelijke hackers die mee willen doen, maar benadruk niet te veel dat ze er zijn want dat is ongemakkelijk. Ga ook niet krampachtig, puur voor de gender balance vrouwen vragen die eigenlijk niet kunnen hacken, want dan bereikt u het tegenovergestelde.

Probeer het aantal aanwezige journalisten te beperken of er in elk geval voor te zorgen dat ze de deelnemende hackers niet te veel lastig vallen. Hetzelfde geldt voor hoge piefen die even worden ingevlogen om met een hacker op de foto te gaan. Niet doen. Dan drukt u bij hackers echt op de verkeerde knop.

Het één op één overnemen van bovenstaande tips is zeker geen garantie voor succes. Ze kunnen echter wel bijdragen aan het neerzetten van een authentiek evenement dat bij uw organisatie en doelstelling past."

trekkelijke, uitdagende, veilige en persoonlijke omgeving creëren waar de kennis en kunde van anderen (de hackers) volledig tot hun recht komen.

Nadat we bij gemeente Den Haag met behulp van partners als Cybersprint en Zerocopter onze basis op orde begonnen te krijgen, hebben we, samen met Cybersprint, een unieke stap gemaakt met het organiseren van Hâck The Hague. Initieel wilden we op deze manier onze Responsible Disclosure (voorloper van Coordinated Vulnerability Disclosure) wereldkundig maken, maar het was zo'n enorm succes dat we het nu elk jaar herhalen. We zijn in 2017 begonnen met een 20-tal hackers en een beperkt aantal eigen systemen en websites die gehackt mochten worden. Inmiddels doen er meer dan 200 professionele en student hackers mee die een groot aantal gemeentelijke systemen en websites onder de loep nemen om te kijken of deze te breken zijn. Daarnaast melden zich elk jaar meer leveranciers van de gemeente aan met hun eigen systemen om de beveiliging ervan naar een nog hoger niveau te krijgen. Verandering is de enige constante en dat geldt zeker ook voor ons jaarlijkse hack-evenement. Hâck The Hague zal in 2021 voor het eerst online worden gehouden, een heel extra nieuwe dimensie.

In het volgende hoofdstuk gaan we meer in detail in op de verschillende aspecten die bij de organisatie van een hack-evenement een rol spelen. Met als doel dat u op basis van deze informatie een vliegende start kunt maken en het wiel niet meer helemaal opnieuw uit hoeft te vinden.

HOOFDSTUK 3
HET ORGANISEREN VAN EEN HACK-EVENEMENT

Net als bij elke andere happening, zit ook bij de organisatie van hack-evenementen de duivel in de details. Zonder een poging te willen doen om volledig te zijn, vindt u in dit hoofdstuk een aantal belangrijke pijlers die de basis vormen van uw hack-evenement. Achtereenvolgens komen de volgende punten aan de orde:

3.1 Bepalen scope en invullen basisvoorwaarden

3.2 Aandachtspunten PR & communicatie

3.3 Voorbereiding

3.4 Uitvoering voorafgaand aan evenement

3.5 Tijdens het evenement

3.6 Nazorg

Bijlage 1 tenslotte beschrijft een hack-evenement draaiboek op hoofdlijnen.

3.1 BEPALEN VAN DE SCOPE EN INVULLEN BASISVOORWAARDEN

Vaststellen van de scope van het evenement

- Datum en duur van het evenement
- Vaststellen fysieke locatie of keuze voor online omgeving (of én én / hybride)
- Aantal hackers en verhouding professioneel / student en vaardigheden. Bij aanmeldingen is het goed om te kijken dat je een variëteit aan hackers hebt. Elke hacker heeft vaak een bepaalde methode of specifieke kennis van een tool. Het is goed daarom goed om aandacht te besteden aan de vaardigheden en het niveau van de hackers
- Inventariseren welke eigen systemen en welke leverancierssystemen je openstelt voor de hackers

Invullen van de basis voorwaarden

- Inventariseren en reserveren benodigde capaciteit vanuit verschillende disciplines
  - Management back-up
  - Projectmanagement
  - Communicatie & PR
  - Security
  - ICT
  - Partnermanagement
  - Leveranciersmanagement
- Bepalen van benodigde systemen
- Uitwerken en reserveren van benodigd budget (direct/indirect)
- Opstellen van kaders
- regels voor deelname
- afstemmen mogelijke juridische implicaties
- Benoemen van de juryleden

3.2 AANDACHTSPUNTEN PR & COMMUNICATIE

Aandachtspunten PR

- Doelstelling PR activiteiten
- Hoofd- en sub-thematieken
- Te betrekken partijen / publicaties
- In te zetten communicatiekanalen voor PR doeleinden (eigen / derden)
- Te creëren content (artikelen, blogs, video’s, podcasts etc.)

Aandachtspunten Communicatie

- Te benaderen doelgroepen
  - Medewerkers eigen organisatie
  - Partners
  - Hacker-community
  - Leveranciers
  - Burgers / publiek / klanten
- Database te benaderen doelgroepen
  - Welke informatie heeft u van elke doelgroep nodig
  - Waar wordt deze informatie vastgelegd
  - Hoe zorgt u ervoor dat deze informatie up-to-date blijft
- Benodigde content per doelgroep
- In te zetten communicatiekanalen per doelgroep (eigen / derden)

3.3 VOORBEREIDING

Coördinatieteam

- Opstellen projectteam
- Inplannen en voorbereiden brainstormsessies
- Hosten brainstormsessies en uitwerken notulen
- Plan van aanpak inclusief planning maken
- Begroting opstellen

Projectteam

- Brainstormen evenement:
  Doel, doelgroep, locatie, deelnemers, stakeholders, intern betrokken, opzet, medium, inhoud wedstrijd, inhoud programma, budget, prijzen

Communicatieteam

- Bepalen van doel en doelgroep
- Uitwerken brainstorm ideeën voor communicatie
- Evalueren wat tijdens vorige edities goed werkte
- Budget bepalen en indelen
- Opstellen planning
- Bijhouden actielijst
- Voorbereiden meetings
- Communicatieoverleg

Techniekteam

- Opstellen plan van aanpak en planning
- Offerte Open VPN licenties
- Ontwerpen dashboarding
- Ontwerpen backend
- Inventariseren laaghangend fruit
- Prepareren tools voor scannen
- Wekelijks teamoverleg
- Schouw locatie
- Inventarisatie benodigdheden IT
- Presentatie Management Team
  Uitvoering & Beheer Hâck The Hague 2021
- Reserveren capaciteit IT-Basisdiensten
- Opstellen planning

3.4 UITVOERING VOORAFGAAND AAN EVENEMENT

Coördinatieteam

- Bijhouden acties
- Opzetten meetings
  - Online platform
  - Benaderen partijen voor bouw platform
  - Demo opvragen partijen
  - Planning platformbouw opvragen
- Programma
  - Opzet programma maken
  - Finaliseren programma inhoud
  - Interviews met sprekers
- Registratie
  - Formulier opbouwen
  - Landing page voor registratie opzetten
  - Nieuwsbrief/Registratie open email
  - Updates naar betrokkenen
  - Selectie 1
  - Selectie 2 (back-up)
  - Email selectie bevestiging deelname
  - Email niet-deelnemers wachtlijst/back-up lijst
  - Tweede ronde bevestiging deelname back-up lijst
- Videoproducent
  - Kick-off video
  - After movie
  - Video’s ter opvulling online programma
  - Editen video’s
  - Maken overgangsbeelden

Projectteam

- Opstellen dagprogramma
  - Programma
  - Inhoud - doel, doelgroep
  - Format
  - Uitvoering
  - Kiezen deelnemers
  - Benaderen deelnemers via e-mail
  - Opname video (voorgesprek, briefing, script, filmen, bewerken, controle, finaliseren)
  - Opname podcast (voorgesprek, opstellen vragen, interview)
  - Opvragen en aanleveren spreker bio en foto voor sprekerspagina
  - Bewerken video en podcast: huisstijl, jingle, ondertiteling, vertaling
- Wedstrijd
  - Deelnemers (aantal landen en ervaring)
  - Prijzen
  - Voorwaarden
  - Regels
  - Opstellen jury
  - Briefen jury
- Regelmatig projectoverleg

Communicatieteam

- Bijhouden actielijst
- Voorbereiden meetings
- Communicatieoverleg
- Draaiboek opstellen
  - Doelgroep hackers
  - Nieuwsbrieven opstellen en versturen
  - Registratieformulier maken
  - Bekers winnaars bestellen
  - Mailen informatie
  - Mailen inloggegevens
- Doelgroep student hackers
  - Inventariseren scholen
  - Gesprekken met scholen
  - Informatiepakket maken (online) Mail opstellen scholen
  - Benaderen scholen
  - Inschrijven scholen
  - Lijst bijhouden aanmelding
  - Selectie hackers
  - Contact opnemen met geselecteerde hackers
  - Logo's opvragen scholen
  - Q&A studenthackers opstellen
  - Communicatieflow hackers vertalen naar studenten
  - Opstellen letter of recommendation
  - Ondertekenen letter of recommendation
- Doelgroep potentiële hackers
  - Aanschrijven platformen voor verspreiding HTH-registratie
  - Social posts
  - Via eigen netwerken van bij organisatie betrokken personen
- Doelgroep leveranciers
  - Testimonials bij leveranciers afnemen
  - Tekst mail leveranciers opstellen (2x)
  - Check mail aan leveranciers
  - Mail aan leveranciers versturen (2x)
  - Beldag inplannen overtuigen leveranciers
  - Mailbox leveranciers bijhouden
  - Opvolging leveranciers versturen
  - Logo's & specs uploaden per leverancier
  - Coördinatie contact leveranciers via één mailbox
  - Dag vooraf link programma + tweetvoorstel mailen
- Doelgroep: burgers voornamelijk door middel van PR
  - Schrijven, reviewen en accorderen persberichten
  - Versturen save-the-date
  - Versturen persuitnodiging HTH21
  - Versturen reminder persuitnodiging
  - Versturen pers Inlog/account info
  - Versturen persbericht na event
  - Monitoring
  - Mediapitches uitschrijven
  - Guerrilla marketing

- Doelgroep: Intern organisatie
  - Aankondiging HTH
  - Plan interne organisatie
  - Dag vooraf link programma + tweetvoorstel mailen
- Podcast
  - Benaderen geschikte mensen voor interview
  - Uitwerken vragen, interviewen (online)
  - Editen podcast
- Video
  - Scripts schrijven
  - Offertes opvragen ondertitelen
- Logistiek & catering
  - Locaties inventariseren en reserveren
  - Catering bestellen
  - Props voor tijdens event (eventaankleding)
  - Datum en tijd woordvoerders vastleggen
  - Checken wie er een dagpas nodig heeft
- Editor
  - Banners maken
  - Aankleding event ontwerpen
  - Landkaart maken van landen die meedoen
  - Prijzencheque ontwerpen

Techniekteam

- Implementatie VPN-oplossing
- Configureren VPN-oplossing
- Testen VPN-oplossing
- Technische oplossing backend
- Testen backend
- Oplossen laaghangend fruit
- Dashboarding opleveren
- Testen dashboarding
- Afstemming Control Room
- Inrichten Discord-kanalen

3.5 TIJDENS HET EVENEMENT

Coördinatieteam

- Programma bewaken
- Aanspreekpunt videoteam

Projectteam

- Algemene vragen
- Beschikbaar voor jury

Communicatieteam

- Beschikbaar voor interne vragen
- Beschikbaar voor persvragen
- Moderator Discord

Techniekteam

- Stand-by voor technische vragen
- Opzetten techniek tijdens event
- Control room
- Moderator Discord

Logistiek & catering

- Catering begeleiden
- Pizza’s bestellen
- Zorgen dat ruimtes beschikbaar zijn
- Begeleiden live interviews

3.6 NAZORG

Coördinatieteam

- Goodie bags versturen
- Evaluatie projectteam opzetten
- Bedankje naar jury sturen

Projectteam

- Evaluatie projectteam evenement en resultaten

Communicatieteam

- Evaluatie evenement en resultaten
- Media coverage verzamelen
- Recensies opvragen bij leveranciers en deelnemers
- Mail opstellen voor deelnemers voor na het evenement (bedankje/ formulier/levertijd/enquête)

Techniekteam

- Oplossing resultaten testen
- Oplossen resultaten scan
- Andere restpunten

Logistiek & catering

- Evaluatie middelen

DANKWOORD

Het succes van afgelopen edities van Hâck The Hague is te danken aan de bijdragen van een groot aantal personen. Niet in het minst die van de deelnemende hackers, maar zeker ook aan het gemotiveerde en enthousiaste kernteam van medewerkers van de twee organisatoren: gemeente Den Haag en Cybersprint. Onderstaand een onvolledige lijst van personen die we met naam en toenaam willen bedanken voor hun aandeel in het realiseren en verder vervolmaken van Hâck The Hague: Asmara Kramer (PPMO Gemeentebrede ICT Portfolio - Gemeente Den Haag), Chantal Stekelenburg (Head of Operations - Zerocopter), Chris van ’t Hof (Presentator, Onderzoeker, Schrijven en Organisator in informatietechnologie), Floor Terra (Senior Privacy Advisor), Letizia Luijs (Communicatie & PR), Liset Metz (Consultant Marketing & Communication - Cybersprint), Marieta van den Heuvel (Communicatieadviseur Informatisering & Automatisering - Gemeente Den Haag), Michel Slootweg (Information Security Officer - Gemeente Den Haag), Peter van Eijk (Information Security Manager - Gemeente Den Haag), Wouter Wouda (Grafisch ontwerper - Cybersprint).

BIJLAGE 1
DRAAIBOEK HACK-EVENEMENT OP HOOFDLIJNEN

INHOUD

Contactgegevens

- Projectteam
- Deelnemers live dagprogramma
- Jury
- Facilitair en AV-media
- Discord moderators

Locatie

- Adres
- Ruimtes
- Catering
- AV-middelen
- Rolverdeling

Programma (beknopt)

Programma + scripts

Wat als scenario's

Smoelenboek

CONTACTGEGEVENS

Projectteam

NAAM & FUNCTIE	E-MAIL & TELEFOONNUMMER
Budgetbeheer	
CISO	
Communicatie	
Coördinatie & pers	
Dagvoorzitter	
Facilitair	
Managementondersteuning	
Marketing	
Techniek	

Deelnemers live dagprogramma

NAAM	TELEFOONNUMMER

Juryleden

NAAM + ORGANISATIE	TELEFOONNUMMER

Facilitair en AV-media

NAAM	TELEFOONNUMMER

Discord moderators

NAAM ISO	INZET ZEROCOPTER	INZET SOCIAL MEDIA
		M
	O	
		O

O = Ochtend
In ieder geval gedurende de ochtend 10:00 – 13:00 uur. Misschien ook in de middag nodig onderling afstemmen.

Dag = Hele dag
Hele dag aanwezig als hulp en ondersteuning.

M = Middag
In ieder geval de middag van 13:00 – 16:00 uur. Misschien ook in de ochtend nodig. Onderling afstemmen.

LOCATIE

Adres

- NAW
- telefoon
- contactpersoon
- routebeschrijving

Ruimtes

- Naam van de ruimte, gebruik van de ruimte
- …
- …

AV-Middelen

- Schermen + bijbehorende HDMI-kabels
- Laptops en locaties waar deze nodig zijn
- Support op de dag zelf zodat de schermen het gewoon blijven doen.

Rolverdeling van personen op locatie

- …
- …

Catering

TIJD	SOORT	LOCATIE
08:00 - 18:00	Koffie en Thee	
10:00	Muffins	
12:00	Lunch	
15:00	Kaasbroodjes	
17:30	Borrel	
18:00	Pizza	

PROGRAMMA (BEKNOPT)

TIJD	FORMAT	ONDERDEEL	WOORDVOERDERS
09:30 - 10:00	Live	Timer die aftelt tot begin HTH	
10:00	Live	... spreekt hackers en bezoekers aan	
10:25	Video	Deel 1/2 Kick-off	
10:27	Video	Deel 2/2 introductie	
10:30	Live	... opent technische briefing voor deelnemers (live)	
10:59	Video	Overgangsscherm	
etc.	etc.	etc.	

PROGRAMMA + SCRIPT

Blok 1: Kick-off

Tijd: **09:30-10:00 (30 minuten)**
Locatie: -
Aanwezig: -
Beeld: Timer die afspeelt

Tijd: **10:00-10:25 (25 minuten)**
Locatie: Studio (foyer)
Aanwezig: Chris, Jeroen, Pieter, Peter
Beeld: Zittend aan tafel. Opening event met …
etc.

Tekst <persoon>

- Welcome all to the first digital version of Hâck The Hague!
- We are live from the city’s town hall.
- […]
- Next to me is …..

Vragen <persoon> aan <persoon>

- A new year of Hâck the Hague. Are you looking forward to it?
- How did Hâck the Hague come so far?
- …..

[….Verder uit te werken voor alle blokken van het programma]

WAT ALS SCENARIO'S

Internet valt weg

Probleem:

Aanpak:

Oplossing:

Team:

YouTube live wordt gehackt

Probleem:

Aanpak:

Oplossing:

Team:

Het uitzendscherm zwart is

Probleem:

Aanpak:

Oplossing:

Team:

Hackers stuiten op zeer gevoelige informatie

Probleem:

Aanpak:

Oplossing:

Team:

VPN werkt niet meer werkt

Probleem:

Aanpak:

Oplossing:

Team:

[…]

V1.0 // NOVEMBER 2021