CONTINUOUS SECURITY

SERVICE SHEET



BROAD HORIZON

CONTINUOUS SECURITY

Elke organisatie is anders. Daarom benaderen we Continuous Security als een werkwijze die uit verschillende fases bestaat: Discover, Onboard en Journey. Door systematisch de drie fases te behandelen, verzamelen we inzichten over de organisatie, doelen en het security maturityniveau van je organisatie. Inzichten die we gebruiken als basis voor het samenstellen van een securityroadmap en een continue samenwerking. We streven hierin om je organisatie naar een volgende securitylevel te krijgen.

De meeste bedrijven zijn tegenwoordig begonnen om de cloud serieus te nemen. Niet iedereen is echter in staat om een robuuste cloudstrategie te bouwen. Vanuit het perspectief van bedrijfsmobiliteit heeft men geen gedetailleerd inzicht in welke gegevens werknemers op hun apparaten opslaan, of bedrijfsgegevens worden gebruikt op onbekende en onbeheerde SaaS-toepassingen, of hoe hun bestanden en gegevens kunnen worden beschermd tegen per ongeluk of opzettelijk verspreiden.

Anderen zijn zich bewust van deze uitdagingen, maar weten niet waar ze moeten beginnen en weten niet zeker hoe klaar hun personeel, systemen, tools en processen zijn voor echte zakelijke mobiliteit. Dit is de reden waarom wij bij Broad Horizon security aanpakken via onze continuous werkwijze.

Discover: In dit proces onderzoeken we de processen, mensen en systemen die zich bevinden in je organisatie en waar de risico's zitten.

Onboard: We maken samen een plan om de securityrisico's te adresseren en om medewerkers te trainen zodat zij de gevaren snel kunnen herkennen.

Journey: We maken een plan om ongoing securitywerk te verrichten zodat we stapsgewijs naar een hoger securityniveau komen.

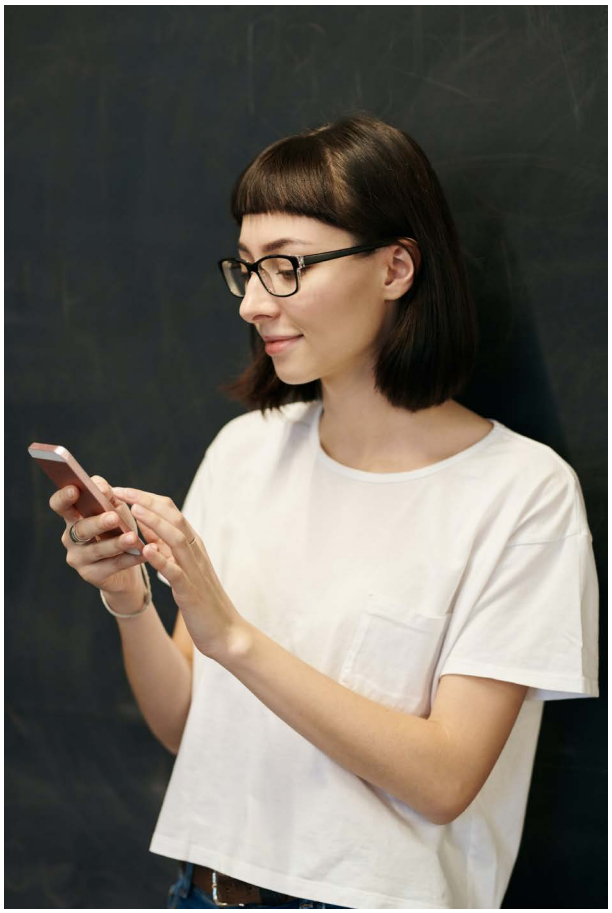
We sluiten deze paper af met een uiteenzetting van onze ongoing Continuous Security diensten: Security Operating Center (SOC), Security Awarenenss en Security Assessment.



1. DISCOVER

Securityrisico's bevinden zich vaak in een klein hoekje. Een verkeerde configuratie in de firewall. Verouderde en daardoor kwetsbare software. Een gebrek aan kennis van medewerkers over hoe ze moeten handelen bij een incident. Of überhaupt het gebrek aan een securitybeleid binnen de organisatie. Het belangrijkste aspect van een securityplan: duidelijk in kaart brengen waar de kwetsbaarheden zich bevinden. Als je dat weet kun je beginnen met het minimaliseren van risico's.

In de Discover-fase brengen we in kaart welke securityrisico's er in jouw organisatie plaats kunnen vinden. We toetsen met een assessment die gebaseerd is op het NIST-framework waar de aandachtspunten liggen. In een rapport geven we vervolgens alle opgedane inzichten een score zodat we zien wat het securitylevel van jouw organisatie is. Aan de hand van het rapport bedenken we een roadmap waarin we de weg schetsen hoe we jouw organisatie naar het volgende securitylevel brengen. We komen tot slot met een onboardingplan waarin we het technologische fundament voor continue security bepalen.



1.1. Assessment

Het kennisniveau over securityrisico's is sterk verschillend van persoon tot persoon. Daarom is het belangrijk om te toetsen hoe medewerkers omgaan in bepaalde scenario's. Dit doen we met een assessment.

Het doel van het assessment is om inzicht te krijgen in de belangrijkste actiepunten. Waar staat de organisatie nu in het Security Maturity Model en welke stappen zijn er nodig om tot een volgend level te komen? Hoe is het kennisniveau van medewerkers op het gebied van security en processen? En wat is de mogelijke impact daarvan op je organisatie?

Het assessment is tweeledig. We stellen individuele medewerkers of groepen medewerkers (bijvoorbeeld op afdelingsniveau) vragen op drie onderdelen: users & devices, applicaties & data en infrastructuur & connectiviteit. Uit dit gesprek halen wij de belangrijkste inzichten en toetsen deze aan het NIST-framework.

Daarnaast voeren wij een digitale scan uit op de applicaties die je organisatie gebruikt. Deze scan onderzoekt op bekende kwetsbaarheden. Denk aan software die verouderd is of aan poorten die niet open mogen staan.

1.2 Adviesrapport

Gewapend met de inzichten uit de interviews en de digitale scan kunnen we aan de slag met het adviesrapport. In dit rapport verzamelen we de inzichten uit het assessment en koppelen deze aan het NIST-framework. Hiermee bepalen we onder andere de impact per gevonden securityrisico en het niveau waarin deze zich bevindt in het Security Maturity Model. Aan het eind van het rapport ontstaat een duidelijk geschreven profiel van waar je organisatie zich nu bevindt in het Security Maturity Model. We sluiten het adviesrapport af met een eerste advies.



1.3 Onboardingplan

Het krijgen van een securityadvies en een bijgevoegde roadmap opent vaak de ogen, maar als je het alleen daarbij laat verdwijnt het advies weer net zo goed in de bezemkast. Daarom sluiten wij de Discover-fase af met een concreet onboardingplan.

In het onboardingplan leggen we alle details vast van de realisatie. We beperken ons hierin niet alleen op het technische fundament dat we in moeten richten en beheren, maar juist ook op de processen die nodig zijn om deze te ondersteunen. We bepalen bijvoorbeeld of het nodig is om periodieke security audits uit te voeren op applicaties en systemen en hoe vaak dit moet gebeuren.

Daarnaast heeft het onboardingplan een sterk menselijk karakter. Omdat veel van de securityfouten afkomstig zijn van menselijke interpretaties, hebben we in het onboardingplan ook uitgebreide aandacht voor het trainen van medewerkers. Ook kunnen we zaken opnemen zoals het gericht uitvoeren van phishingaanvallen.

Een belangrijk onderdeel van het onboardingplan is de roadmap – een stappenplan die is afgestemd aan het optimaliseren van security binnen jouw organisatie. Hierin leggen we vast welke stappen we moeten zetten om samen naar het volgende securitylevel te komen.



2. ONBOARD

Het inrichten van een nieuw securityprogramma gaat verder dan het configureren van software. Vaak zijn er meerdere stakeholders bij betrokken met verschillende kennisniveaus over security Daarom letten wij tijdens de onboarding van het securityprogramma niet alleen op het inrichten van technologie, maar ook op het toetsen van het kennisniveau. We zijn van mening dat iedereen binnen de organisatie dezelfde basisvaardigheden moet bevatten over het signaleren van securityrisico's.

Met een awareness-training helpen we om dit het bewustzijn van security binnen de organisatie op hetzelfde niveau te brengen. Naast het trainen van medewerkers voeren we security audits uit op de belangrijkste bedrijfsapplicaties, waar we op zoek gaan naar kwetsbaarheden in de omgeving. Deze kwetsbaarheden ontvang je in een duidelijk omschreven rapport inclusief de impact per gevonden kwetsbaarheid en de oplossingsrichting.

2.1 Inrichting

In dit stadium richten we de technologie in die nodig is om je bedrijf veilig te houden. Denk aan het implementeren en inrichten van nieuwe firewalls, het toepassen van een Mobile Device Management oplossing of de installatie van monitoringsoftware waarmee we de mogelijke risico's voor jouw omgeving in de gaten houden. Welke technologie we gebruiken hangt sterk af van de keuzes die we eerder hebben gemaakt in de Discover-fase en in de roadmap die we daarop hebben afgestemd.

2.2 Awareness

Een van de meestvoorkomende inzichten is dat het bewustzijn van iedereen in de organisatie moet worden vergroot.

Binnen Continuous Security doen we dat met een awareness-training. Dit is een training die gebaseerd is op jarenlange best-practices van de security engineers die bij Broad Horizon in dienst zijn. Zij weten als geen ander wat er fout kan gaan. In heldere communicatie trainen wij medewerkers vanuit alle lagen van de organisatie zodat er meer bewustwording wordt en iedereen de basis van een aanval kan signaleren.

Aanvullend op de training kunnen we ook phishingaanvallen uitvoeren. Dat zijn aanvallen die gericht zijn op medewerkers via de mail te misleiden. Het lijkt alsof de mail afkomstig is van een betrouwbare partij, maar er staat uiteindelijk een malafide link in. Als medewerkers op deze link klikken kunnen we in potentie malware installeren. Dat doen we natuurlijk niet, maar we verzamelen wel de statistieken van medewerkers die erop klikken. Zo krijg je inzicht in de aantallen medewerkers die vatbaar zijn voor een phishingaanval. In de training is er overigens volop aandacht voor phishing: hoe herken je een phishingmail en wat moet je doen als je er (al dan niet per ongeluk) op reageert.

"AANVULLEND KUNNEN WE OOK PHISHING-AANVALLEN UITVOEREN"

2.3 Optimalisaties

De inzichten die we halen uit de awareness-training en de security audit gebruiken we om verdere optimalisaties door te voeren. Dat kan bijvoorbeeld zijn dat we meer mensen binnen de organisatie trainen of dat we afspreken om periodiek een security audit uit te voeren op de belangrijkste systemen.

3. JOURNEY

Binnen traditionele securitymodellen was het vaak voldoende om security centraal in te regelen. Wijzigingen vonden weleens plaats, maar omdat applicaties en systemen vanuit een on-premise omgeving werden gehost, was het doorvoeren van die wijzigingen overzichtelijk.

Met de komst van cloudapplicaties en nieuwe ontwikkelmethodieken is het doorvoeren van wijzigingen iets wat continu gebeurt, en vaak ook nog over verschillende gedistribueerde systemen. De snelheid waarmee wijzigingen plaatsvinden en het groeiende aantal cloudapplicaties en data vraagt om een andere securityaanpak.

Daarom benaderen we security vanuit een continu proces. Binnen Broad Horizon geloven we dat je regelmatig terug moet keren naar de tekentafel, bijvoorbeeld als je nieuwe technologie introduceert binnen de organisatie of als er nieuwe kwetsbaarheden in het spel komen kijken.

Binnen de Journey-fase van Continuous Security kijken we daarom met een brede blik naar online veiligheid – het is nooit af omdat er altijd wel iets te verbeteren valt.

Je zal regelmatig terug naar de tekentafel moeten, bijvoorbeeld als je nieuwe technologie in je organisatie omarmt of als er een nieuw securitylek bekendgemaakt is. Afhankelijk van de afspraken die je met ons maakt keren voeren wij periodiek assessments en awarenesstrainingen uit.

Ook kunnen wij met onze Securtity Operating Center signaleren waar mogelijke risico's zijn.

Bij grote nieuwe gevaren updaten we snel via bestaande communicatiekanalen wat de impact is voor uw organisatie.



4. ONZE DIENSTEN

Na de uitgebreide werkwijze hebben we inzicht in het securityniveau van jouw organisatie en een duidelijke roadmap. We weten heel duidelijk welke (Microsoft) technologie we in kunnen zetten en of er sprake is om nieuwe licenties aan te schaffen. Daar stopt Continuous Security echter niet. Naast het leveren van diensten op het gebied van infrastructuur & connectivity, applications & data en users & devices zijn de volgende pilaren altijd aanwezig binnen Continuous Security:

- Security Operations Center (SOC)
- Security Awareness
- Security Assessment

Security Operations Center (SOC)

Intelligente securitymonitor
Bij het groeien van de digitale omgeving van jouw bedrijf, groeit ook het risico van cybercriminelen. Een aanval heeft nadelige gevolgen voor het vertrouwen, klanten en omzet. Daarom is het taak dagelijks grip te houden op de veiligheid.

Tegenwoordig is het simpel aan- of uitzetten van producten en diensten vanuit de Microsoft licentie(s) niet genoeg om deze veiligheid te waarborgen. Juist om deze reden is het belangrijk om veel gegevens te verzamelen en verbinding te maken vanuit alle systemen, ongeacht of deze in de Cloud of on-premise zijn.

Echter is het aansluiten van alle producten en diensten niet simpel, dit kost veel resources en brengt ook de nodige uitdagingen met zich mee. Een enorme operationele bezetting die vaak niet goed te sturen is, mede omdat de systemen niet schaalbaar zijn en het hierbij om enorme datavolumes gaat. Het gevolg is dat dit enorm kostbaar wordt en veel onnodige waarschuwingen laat zien.

Daarom heeft Broad Horizon een lightweight SOC (Security Operations Center) ontwikkeld om aan de vier meest belangrijke beveiligingsactiviteiten te voldoen:

Verzamel
Het doelbewust verzamelen van data(volumes) op schaal, met focus op gebruikers, apparaten en applicaties, zowel on-premise als in de private cloud. Dit betreft dus data over producten, technologie en diensten die jouw bedrijf gebruikt binnen de IT-omgeving.

Detecteer
Met onze lightweight (intelligente) SOC ontdekken wij sneller bedreigingen en minimaliseren zogenaamde onnodige waarschuwingen (false-positives) met behulp van grote datavolumes en een intelligent tools (Sentinel) en bedreigingsinformatie van Microsoft.

Onderzoek
Bedreigingen worden met AI (Artificial Intelligence) snel opgemerkt en op proactieve- en grootschalige wijze verdachte activiteiten geblokkeerd. Hierbij draagt de jarenlange kennis van onze Security Specialisten aan mee om dit met succes uit te voeren.

Reageer
Binnen onze systemen wordt er adequate manier op incidenten gereageerd. Veelal via automatisering en workflows (werkstromen) kunnen wij op grote schaal zorgen dat wij meer tijd hebben om ons te concentreren op de echte beveiligingsproblemen binnen jouw bedrijf. Als je de beveiliging van jouw bedrijf wilt verbeteren overweeg dan de SOC-diensten van Broad Horizon. Met deze dienst hebben wij een enorme toegevoegde waarde in de beveiliging van jouw organisatie.

Security Awareness

Security incidenten vinden vaak plaats bij en via medewerkers. Dit kan bijvoorbeeld bij malware uitbraken of CEO-fraude komen door het verkeerd behandelen van mail. Vaak kan een gebruiker wel de meest basale trucjes van hackers herkennen. Echter valt men snel door de mand op het moment dat er een gerichte actie plaatsvindt.

Om gebruikers de laatste technieken en methodes te laten ervaren en een gezonde hoeveelheid wantrouwen te kweken voeren wij phishingcampagnes uit. Hierbij maken we een gepersonaliseerde aanval via de mail waarbij we bijvoorbeeld gebruikersgegevens of accounts willen overnemen.

Door deze mails goed opgezet en met de hand te maken kunnen we zo het slagingspercentage van onze aanval vergroten. Uiteindelijk is het doel de gebruikers meer bewust te maken van de risico's en tevens ook een real-life scenario te geven waarbij men weet welke stappen men dient te ondernemen. Na afloop krijgt u een rapport waarbij genoteerd staat wat we hebben uitgevoerd en de successen die erbij zijn behaald. Daarnaast een advies om dit soort type aanvallen tegen te houden of de impact te verkleinen. Het is immers zo dat het eerder mogelijk is de impact zo klein mogelijk te krijgen dan ervoor te zorgen dat het niet plaatsvindt.

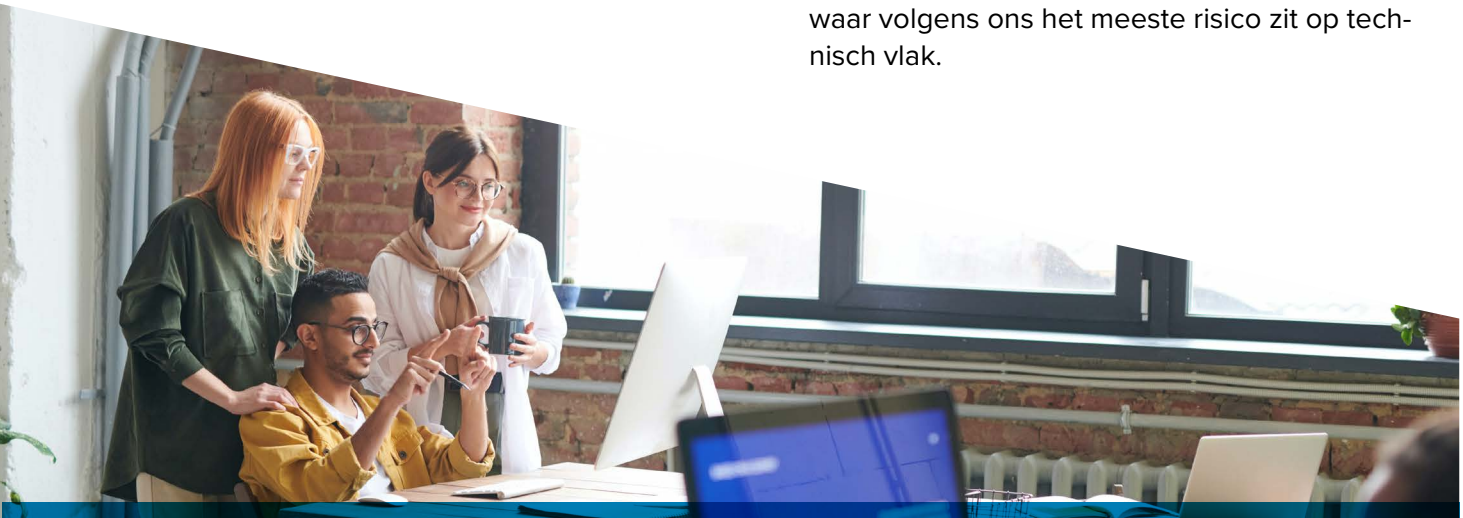
Security Assessment

Om ervoor te zorgen dat een organisatie zo efficiënt blijft functioneren is het noodzakelijk om regelmatig te kijken waar jouw bedrijf staat en waar we naar toe willen. Bij het vraagstuk security is dat niet anders, dit is een continue ding. Er zullen keuzes gemaakt dienen te worden waarop de focus komt te liggen en waar het geld naar toe gaat.

Het maken van deze keuzes is onmogelijk zonder de juiste informatie en goede sturing. Daarom willen we dit gezamenlijk maken. Door middel van een workshop, scan en rapport kunnen we gezamenlijk een roadmap ontwikkelen die de grootste problemen zo efficiënt mogelijk oplossen op de plekken die het meeste impact hebben.

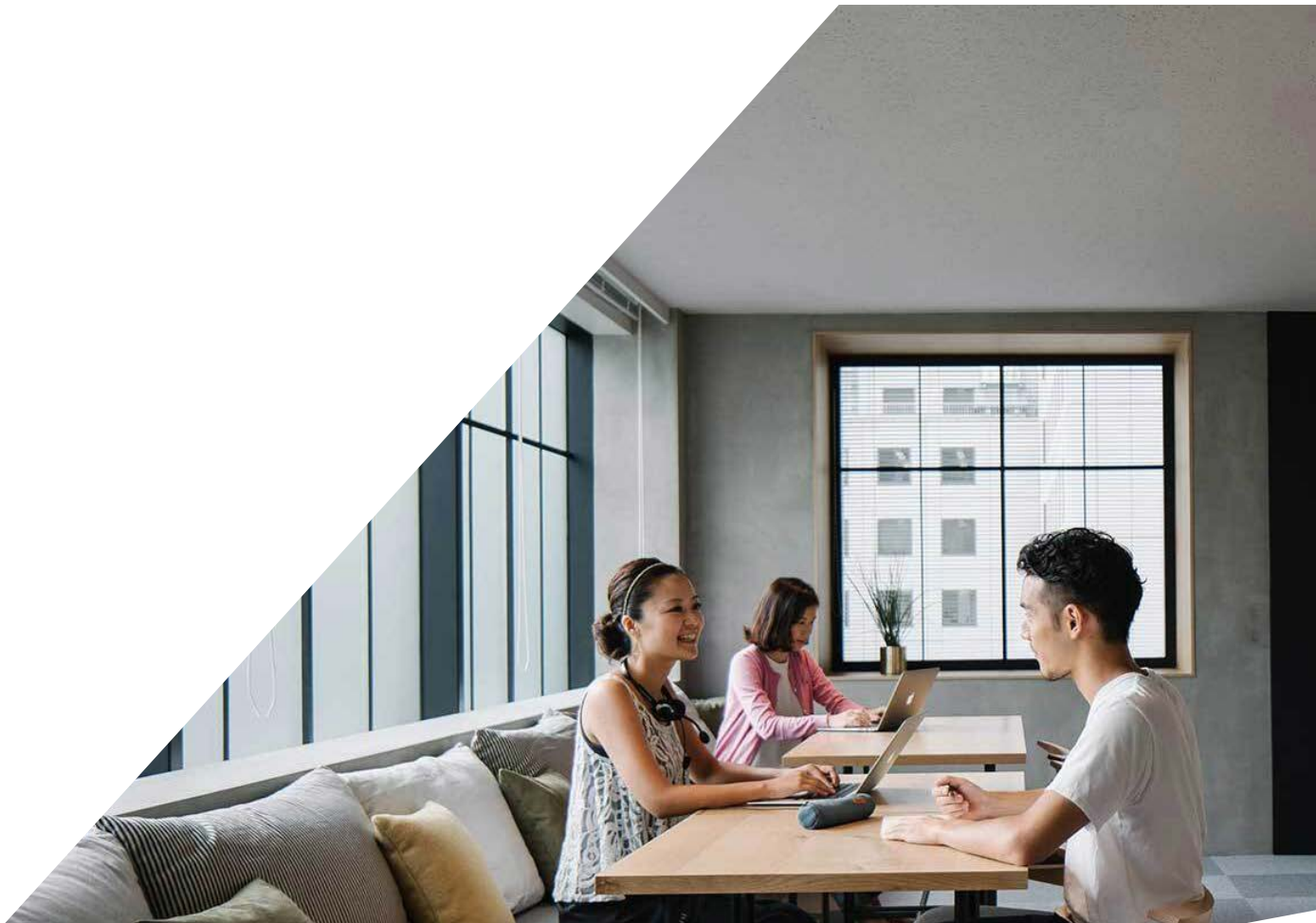
Met de workshop kijken we gezamenlijk naar hoe het vraagstuk van security momenteel is ingeregeld bij het bedrijf. Zo komen we zowel achter het stuk technisch als procesmatig. Immers is niet alleen het technische personeel met de toegang tot de systemen die schade kunnen brengen. Ook de sales afdeling of zelfs het kantine personeel kan voor voldoende ellende zorgen (al dan niet indirect). Door middel van de workshop creëren wij awareness en kijken we door lagen van de organisatie heen naar de huidige middelen en of het bekend is wat de juiste respons dient te zijn.

Naast de workshop komen we op locatie (of wanneer benodigd op afstand) een scan doen om te kijken wat volgens ons de realiteit is. Wat kunnen onze hackers bij jullie naar boven halen en waar liggen volgens ons de pijnlijke punten? Waar kan een standaard gebruiker allemaal bij en hoe zit het met de software updates? Door middel van e en black- en/of greybox audit maken wij een overzicht van waar volgens ons het meeste risico zit op technisch vlak.



Met de uitslagen van de workshop en de scan maken we een rapport waarin alles samengevat wordt. Hierbij kijken we dan ook naar de oplossingen en wat wij nog meer voor jullie kunnen betekenen in de dienstverlening. Gezamenlijk kunnen we dan kijken welke oplossingen er op een roadmap kunnen. Hiermee stellen we met het beschikbare budget een aantal doelen samen die we over tijd heen kunnen plotten. Zo kunnen we efficiënt en met beperkte middelen de meeste impact maken.

Vervolgens kunnen we na een bepaalde tijd weer starten met een nieuwe scan en workshop. Kijken of we de verbeteringen door de organisatie heen kunnen zien en een nieuw plan maken om zo met hernieuwde inzichten de volgende risico's op te pakken. Zo zorgen we ervoor dat met de nieuwste technieken en de juiste risico bereidheid u geen meer risico loopt of geld uit geeft dan noodzakelijk.



Broad Horizon - Being Ahead

Als organisatie wil je vooroplopen, vernieuwen en continu kunnen verbeteren. Doordat de wereld om ons heen constant verandert, moet jouw organisatie wendbaarder zijn dan ooit. Broad Horizon helpt hierbij door op basis van slimme data-inzichten, uitgebreide industriekennis en een volledig dienstenportfolio, bestaande en toekomstige vraagstukken van organisaties op te lossen. Wij zorgen ervoor dat onze klanten altijd een stap vooroplopen.
https://www.broadhorizon.nl

“ ENVIRONMENTS CAN CHANGE AT ANY MOMENT. BUT IF YOU ANTICIPATE, THESE CHANGES WILL OPEN UP UNEXPECTED POSSIBILITIES”

Dave Canterbury
Pathfinder

Keienbergweg 100, 1101 GH Amsterdam – +31 88 008 3500

BROAD HORIZON