Crisis en Resilience

Onverwachte cyberincidenten kunnen uw bedrijf hard raken. Goede voorbereiding is daarom essentieel. Steeds meer bedrijven zien de noodzaak om te anticiperen op cyberincidenten, zodat belangrijke diensten kunnen blijven draaien. Wij kunnen u helpen uw organisatie voor te bereiden.

Deze Crisis en Resilience Diensten geven u:

Inzicht op meerdere niveaus

U krijgt op alle gebieden inzicht in de veerkracht van uw organisatie, zodat u een compleet beeld krijgt.

Realistische simulaties

U oefent met gesimuleerde, realistische cyberaanvallen, gebaseerd op dreigingsinformatie.

Een internationale partner

U profiteert van onze ervaring met klanten over de hele wereld, van multinationals tot overheid.

Waarom Crisis en Resilience Diensten?

Ervoor zorgen dat uw organisatie kan blijven opereren tijdens een cybercrisis is een uitdaging.

- Hoe zorgt u ervoor dat uw medewerkers hun rol en verantwoordelijkheden kennen tijdens een crisis?
- Hoe weerbaar zijn uw kritieke diensten in het geval van ernstige maar aannemelijke incidenten?
- Hoe kunt u uw kritieke diensten blijven leveren in het geval van een cyberaanval?
- Hoe kunt u uw reactie op een cybercrisis oefenen?

Met een goed opgezet Crisis en Resilience-programma kan uw organisatie anticiperen en reageren op nieuwe digitale dreigingen. Zo'n prgramma helpt u ook om te voldoen aan nieuwe EU-cybersecuritywetgeving, zoals **NIS2** en **DORA**, evenals de **FCA/PRA**-regelgeving op het gebied van operational resilience die geldt in het Verenigd Koninkrijk. Wij hebben ruime ervaring met het helpen van klanten met hun crisis management. Laat ons u helpen.

De Crisis en Resilience Diensten die wij bieden

- Crisis Management
- Operational Resilience
- Business Continuity Management
- Cyber Crisis Oefeningen

Crisis Management Diensten

Veel organisaties richten zich bij een cyberincident op de technische respons. Maar is uw organisatie voorbereid op de bredere crisis die vaak volgt? Wij kunnen u helpen bij het ontwerpen en implementeren van kaders, plannen, draaiboeken en procedures voor Crisis Management, of u helpen om lessen te trekken uit een cyberincident. Dit geeft u:

- Inzicht in de volwassenheid van uw crisismanagementraamwerk en in de maatregelen die nodig zijn om aan te sluiten bij internationale normen.
- Een ingebed kader voor crisisbeheer, dat is afgestemd op de internationale crisisnorm ISO 22361.
- Een beproefd crisisresponsprogramma, zodat u niet wordt verrast in het geval van een ernstig cyberincident.

Operational Resilience Diensten

Operationale weerbaarheid is cruciaal om ervoor te zorgen dat uw bedrijf kan blijven draaien in het geval van een cyberaanval of technische storing. Een operational resilience programma geeft u de juiste hulpmiddelen om te anticiperen en te reageren op digitale dreigingen. Dit kan bijvoorbeeld door **Cyber Impact Tolerance Testing**.

Cyber Impact Tolerance Testing

1	Wij onderzoeken uw kritieke applicaties, om vast te stellen welke impact kwetsbaarheden hebben op de weerbaarheid van uw diensten.
2	Wij creëren scenario's voor uw medewerkers, zodat zij kunnen laten zien hoe ze het herstel van belangrijke bedrijfsdiensten garanderen.
3	U ontvangt een rapport met de bevindingen. Dit bevat ook aanbevelingen, zodat u de weerbaarheid van uw belangrijke diensten kunt verhogen.

Business Continuity Management

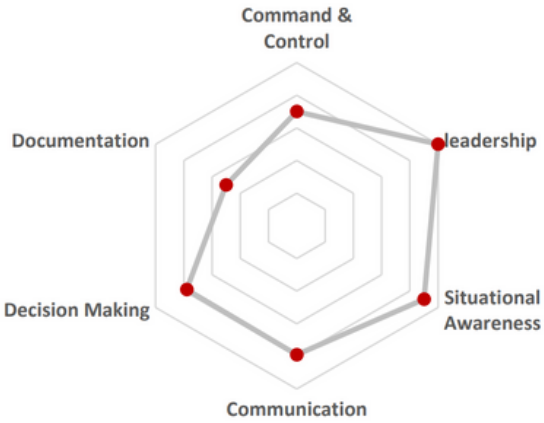
Continuïteit van kritieke diensten is essentieel voor de levensvatbaarheid van uw organisatie. Wij kunnen u helpen met het ontwerpen van een Business Continuity Management System (BCMS) dat voldoet aan de internationale norm ISO 22301:2019.

Krijg inzicht in de diensten van uw organisatie en de middelen die u nodig heeft om te garanderen dat uw kritieke processen kunnen doorgaan in geval van verstoring.

Creëer en test betrouwbare en plannen met herstelstrategieën voor uw personeel, die hen helpen met het kritieke bedrijfsfuncties.

Cyber Crisisoefeningen

Een cybercrisis vraagt niet alleen om een technische respons, maar om een afgestemde reactie van de hele organisatie. Hoe sluit uw strategische respons aan op uw operationele technische respons? Wat verwachten mensen van elkaar? Hoe kunt u na het vaststellen van de aanval snel overgaan tot strategische besluitvorming? Een **Cyber Crisisoefening** helpt u bij het oefenen van uw respons op operationeel, tactisch en strategisch niveau.



Krijg inzicht in de capaciteiten van uw organisatie als het gaat over crisisrespons.

Geef uw medewerkers de kans om hun crisisplannen te oefenen en goed te testen.

Wat onze klanten zeggen

“Deze oefening was goede training”

“De Cyber Crisisoefening die we deden was goed opgezet en helemaal toegesneden op onze situatie. Het gaf daardoor een realistische totaalbeleving.”

De juiste Crisisoefening kiezen

Afhankelijk van wat u nodig heeft, uw doelgroep en uw doelen, kunnen we u helpen met verschillende oefeningen. We bieden ook oefeningen die speciaal zijn ontworpen voor OT-systemen.

Crisisoefeningen

Walk-through	Tijdens deze simpele oefening volgen deelnemers een scenario met een vast stramien en discussies.
Tabletop	Deze realistischere oefening bevat nagebootste scenario-updates. Het crisisteam reageert hierop.
Functioneel	Een oefening met een duidelijk doel, zoals het testen van tooling of communicatieverbetering.
LIVE - Full scale	De meest realistische oefening, met meerdere responsteams en een langere looptijd.
Gold-Teaming	Deze strategische en tactische oefening gebruikt de resultaten van red teaming of pentesting en is gebaseerd op daadwerkelijke aanvalspogingen.

Secura
A BUREAU VERITAS COMPANY

Over Secura / Bureau Veritas

Secura is een toonaangevend cybersecuritybedrijf. Ons doel is om uw cyberweerbaarheid te vergroten. Onze klanten variëren van overheid en zorg tot financiën en industrie. Secura biedt technische diensten aan, zoals vulnerability assessments, penetratietesten en red teaming. We bieden ook audits, forensische diensten en awarenesstrainingen aan.

Secura is onderdeel van Bureau Veritas (BV), een beurs-genoteerde onderneming die gespecialiseerd is in testen, inspecteren en certificeren. BV is opgericht in 1828, heeft ruim 80.000 medewerkers en is actief in 140 landen.

Voorbeeld | Crisis en Resilience

Welk probleem had de klant?

Een internationale fabrikant van verlichting wilde begrijpen welke impact een ransomware-aanval zou hebben op hun fabrieken en hoe hun crisisteams zouden samenwerken om de respons te coördineren.

Resultaat

We hebben voor deze klant een aantal Cyber Crisisoefening ontworpen, afgestemd op hun wereldwijde vestigingen. Hiermee trainden ze hun responsteams en ontdekten ze een aantal mogelijkheden voor verbetering.

BUREAU VERITAS 1828

Meer weten?

Neem contact met ons op om uw cyberweerbaarheid te verhogen.

info@secura.com

+31 (0) 88 888 3100