CTAC
ENABLING YOUR AMBITION

DIGIMIJ
UW STRATEGISCHE IT-PARTNER

DE GREENBOX:
HET PLAN VOOR HERSTEL NA EEN RAMP

Stel je voor dat je door een ramp wordt getroffen waarna geen enkel IT-systeem nog veilig of zelfs bruikbaar is. Wat zijn dan de stappen om zo snel mogelijk de kernactiviteiten op te kunnen starten en weer operationeel te geraken? Is er voor dit soort scenario's vroegtijdig en voldoende nagedacht om onnodige bedrijfsstilstand te voorkomen? Zijn de plannen en alle benodigdheden die destijds bedacht zijn nu ook nog van toepassing?

Rampen

Digimij is op een vrijdagnacht in 2020 getroffen door een brand. "Na 23 jaar zagen wij het bedrijf in vlammen opgaan en stonden wij hier machteloos bij te kijken. Gelukkig hadden we vooraf al maatregelen getroffen voor een dergelijk rampscenario. Deze voorbereiding zorgde ervoor dat we snel weer operationeel waren, met minimale consequenties voor onze klanten. Wat hadden wij gedaan als we niet voorbereid waren en vanaf nul hadden moeten beginnen?"

Hier ontstond de Greenbox. Het idee om te bepalen wat er na een ramp nodig is om zo snel mogelijk weer de bedrijfsvoering te kunnen voortzetten. De kans op een brand is misschien niet al te groot, maar een ransomware aanval is tegenwoordig aannemelijk (steeds vaker in het MKB) met vaak desastreuze gevolgen. Dezelfde maatregelen zijn hierop van toepassing.

CTAC
ENABLING YOUR AMBITION

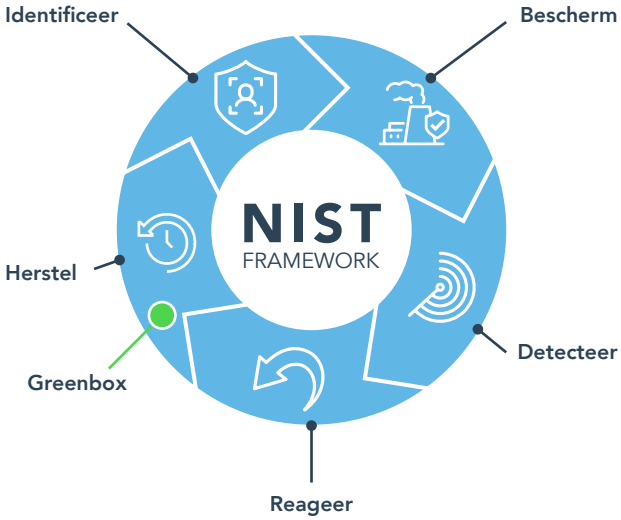
DIGIMIJ
UW STRATEGISCHE IT-PARTNER

De Greenbox

De Greenbox is een dienst waarbij we starten met het inventariseren en vastleggen van de belangrijkste bedrijfsprocessen en vervolgens bepalen we wat nodig is om te zorgen dat deze weer operationeel raken. We analyseren de IT-infrastructuur, de belangrijkste applicaties en de meest cruciale benodigde data. We werken aan een actieplan en de rolverdeling voor de betrokkenen. Het uitgangspunt is een rampscenario waarbij alle IT-middelen verloren zijn.

Al hetgeen ervoor nodig is om operationeel te geraken komt fysiek in de Greenbox en deze dient op een veilige plaats bewaard te worden. Het proces om tot de inhoud te komen herhalen we periodiek en updaten we waar nodig.

Het achterliggende gedachtegoed positioneren wij in de herstelfase na een incident. We werken met het NIST-framework principe wat bestaat uit 5 pilaren om tot een succesvolle securitystrategie te komen. De Greenbox krijgt hiermee een plek in de Herstel pilaar van het framework.



Hoe ziet dit proces eruit?

1. **Intake**
   Tijdens de intake gebruiken we een inventarisatielijst. We kijken, met betrokkenheid van de benodigde stakeholders, naar de bedrijfsprocessen en we bespreken of de reeds getroffen securitymaatregelen een goede basis vormen.

2. **Advies**
   Op basis van de intake stellen we samen een plan op en bepalen we de benodigde middelen om te kunnen herstellen na een ramp. Om de kans te verkleinen dat een IT-ramp überhaupt plaats zal vinden en omdat we een steeds beter inzicht hebben gekregen van de IT-infrastructuur, zullen we ook securityadviezen geven.

3. **De Greenbox**
   Het fysieke product wat hieruit komt is de Greenbox. Een koffer met hierin de meest cruciale benodigd-heden om direct na een ramp te kunnen schakelen en de besproken processen weer in gang te zetten.

4. **Periodieke update**
   Samen bepalen we wanneer de Greenbox geüpdatet dient te worden. Aanvullend bepalen we of de inhoud nog voldoet aan de huidige situatie en passen aan waar nodig.

Wil je meer weten over de Greenbox en ontdekken wat dit voor je organisatie kan betekenen?
Neem contact met ons op. Wij helpen je graag en kunnen je van verdere details voorzien.