

31-5-2024

Versie: 1.0

# Winfra-CERT

## Projectgroep

ICTAISc

## Docent

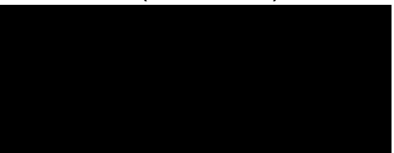


## School en Opleiding

Windesheim Zwolle HBO-ICT Software Engineering, Business IT Management & Infrastructure Design & Security

## Student

Bark, Ivan (s1169347)



Geen vertrouwelijke behandeling gewenst.

## Versiebeheer

Versie	Datum	Omschrijving	Opmerkingen
0.1	21-03-2024	Eerste concept	CERT-bestand aangemaakt
1.0	25-03-2024	Afmaken	CERT afgerond

## Distributie

Naam	Functie	Versie	Datum toezending	Reden toezending
	Docent	1.0	31-05-2024	Oplevering

## Inhoudsopgave

---

1. Inleiding .....	3
2. Aanleiding .....	3
3. Contact gegevens .....	4
4. Rollen .....	5
Bibliografie .....	6

## 1. Inleiding

---

Winfra vital verzorgt de levering van gas en elektriciteit aan klanten in Noordwest Overijssel. De infrastructuur van Winfra vital wordt gezien als een vitale infrastructuur dat met uitval grootschalige maatschappelijke ontwrichting kan veroorzaken, hierdoor is het van belang dat de veiligheid hiervan nauwlettend in de gaten wordt gehouden.

Inlichtingendiensten hebben gewaarschuwd dat vitale infrastructuren steeds meer aandacht krijgt van overheidsactoren. Deze actoren zijn instaat om niet alleen de technische zwakheden te verkennen, maar richten zich ook op kantoorautomatisering en het personeel. Door een snelle digitalisering van deze sector is een structurele aanpak van cybersecurity vereist namelijk: security by design.

## 2. Aanleiding

---

Er wordt een “Security Emergency Response Team” CERT opgesteld. Dit is een team dat is samengesteld om snel te reageren in noodsituaties met betrekking tot informatiebeveiliging. Bij het CERT ligt de verantwoordelijkheid voor het coördineren van de respons van cyberincidenten en het brengen van adviezen gebaseerd op risicoanalyses om zulke incidenten te voorkomen.

Het is van cruciaal belang dat dit document wordt getest en verder wordt afgestemd. Het niet navolgen en verbeteren van dit document kan resulteren in foutief response op een cyber security disaster, wat meestal gepaard gaat met veel verloren tijd, middelen en geld. Om dit dus te voorkomen moet dit document nageleefd worden.

Door het CERT regelmatig in actie te testen en af te stemmen heeft meerdere belangrijke voordelen, ten eerste zijn de mensen waaraan de rollen zijn erkend dan meer ervaren met de verschillende incidenten. Mocht het incident dan echt plaatsvinden, weten ze veel beter hoe ze het probleem kunnen oplossen. Ten tweede worden dan ook mogelijke fouten of verbeterpunten ontdekt in het CERT. Hierdoor zijn de CERT'ers nog beter voorbereid voor een echt security incident.

### 3. Contact gegevens

---

Dit zijn de contactgegevens van de medewerkers binnen het bedrijf die bij het CERT horen. Er wordt verwacht dat CERT leden tijdig beschikbaar zijn, met name voor incidenten in de hoogste urgentie.

Persoon	Email	Telefoonnummer
Ivan Bark		

Er is ook gekozen om een bedrijf in te huren extern die ervoor zorgt dat er altijd een contactpersoon is voor als iemand ziek is of afwezig is vanwege vakantie. Dit bedrijf kan dan bereikt worden om de taken van de CERT over te nemen.

Bedrijf	Email	Telefoonnummer
CERT-huring	Cert@hotmail.com	0621340568

## 4. Rollen

Rol	1 <sup>e</sup> persoon	2 <sup>e</sup> persoon
Team leider	Ivan	Buiten besteed
Incident manager		Buiten besteed
1 <sup>e</sup> onderzoeker		Buiten besteed
Communicatie en PR		Buiten besteed
Juridisch		Buiten besteed
Human resources		Buiten besteed

### Teamleider

De teamleider heeft als belangrijkste taak dat de communicatie met betrekking tot het incident naar de stakeholders goed gaat. Verder zorgt de teamleider ervoor dat er passende aandacht en budget komt vanuit hoger management.

### Incident manager

De incident manager zorgt voor het coördineren van de acties tijdens het incident, zoals het overleg inplannen en checken dat ieder teamlid zijn taak doet. Verder zorgt de incident manager voor periodieke rapportage voor de stakeholders en wordt de communicatie tussen de teamleider en de rest van het team gecoördineerd door de incident manager.

### 1<sup>e</sup> onderzoeker

De onderzoeker is verantwoordelijk voor het onderzoeken van events tijdens een incident. Deze persoon werkt vaak met ander security analisten. De rol van onderzoeker wordt vaak gevuld door een incident responder of security analist uit het SOC-team.

### Communicatie en PR

Dit teamlid is verantwoordelijk voor het monitoren van sociale media, persberichten en het opstellen van berichten naar medewerkers, klanten of leveranciers.

### Juridisch

Dit teamlid houdt zicht bezig met rechtszaken of schadeclaims vanuit het incident. Ook is deze rol verantwoordelijk voor het controleren van alle berichten die naar buiten gaan naar aanleiding van het incident.

### Human resources

Deze rol kan toegevoegd worden als er sprake is van zaken met gevolgen voor het dienstverband van medewerkers of een mogelijke insider threat. Deze persoon is een HR-medewerker die dan verantwoordelijk is voor de medewerkers binnen de organisatie tot betrekking met het incident.

## Bibliografie

---

Cissp, W. S.-. S. I. G. I. G. I. G. I. (2020, 8 februari). *Hoe bouw je een Computer Security Incident Response Team?* <https://nl.linkedin.com/pulse/hoe-bouw-je-een-computer-security-incident-response-wouter>