

31-5-2024

Versie: 1.0

Disaster Recovery Plan

Projectgroep

ICTAISc

Docent

[Redacted]

School en Opleiding

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

Student

Bark, Ivan (s1169347)

[Redacted]

Geen vertrouwelijke behandeling gewenst.

Versiebeheer

Versie	Datum	Omschrijving	Opmerkingen
0.1	17-3-2024	Eerste concept	N.v.t.
1.0	19-3-2024	Tweede concept	Verwerking feedback

Distributie

Naam	Functie	Versie	Datum toezending	Reden toezending
	Docent	0.1	19-3-2024	Verkrijgen feedback
	Docent	1.0	31-05-2024	Oplevering

Inhoudsopgave

Begrippenlijst.....	3
1. Inleiding	5
2. Inventarisatie.....	6
2.1. IT	6
2.2. OT.....	6
3. RPO & RTO.....	7
4. Preparation.....	8
4.1. Policy.....	8
4.2. Response plan/strategy	9
4.3. Communication	10
4.4. Documentation	10
4.5. Team.....	10
4.6. Tooling.....	10
4.7. Training	11
5. Identification	12
6. Containment	13
6.1. Malware	13
6.2. DDoS	13
6.3. Phishing	13
6.4. Inside Threat	13
7. Eradication	14
7.1. Malware	14
7.1.1. Ransomware: Betalen van losgeld	14
7.1.2. Zelf regelen.....	14
7.2. DDoS	14
7.3. Phishing	14
7.4. Inside Threat	15
8. Recovery	16
8.1. Malware	16
8.2. DDoS	16
8.3. Phishing	16
8.4. Inside Threat	16
9. Lessons Learned.....	17
Bibliografie	18

Begrippenlijst

Nr.	Begrip	Betekenis
1.	<u>Back-up</u>	Is een kopie van bestaande systemen en/of data
2.	<u>Inside Threat</u>	Een account welke onbekende kwaadaardige bedoelingen heeft
3.	<u>Malware</u>	Kwaadaardige software
4.	<u>Phishing</u>	Een onschuldig-lijkend bericht waarbij links of bestanden zijn meegestuurd die malware bevatten
5.	<u>DDoS</u>	Distributed Denial-of-Service; Wanneer meerdere systemen tegelijkertijd het netwerk van een bepaalde dienst overbelasten
6.	<u>Firewall</u>	Een lijst met regels die aangeven welke IP-adressen en poorten wel of niet gebruikt mogen worden
7.	<u>Antivirus</u>	Software wat malware analyseert, detecteert en verwijdert
8.	<u>Pentest</u>	Penetratie test; Een oefening om de IT-beveiliging te testen
9.	<u>Segmentatie</u>	Het opsplitsen van het netwerk zodat verschillende diensten niet met elkaar kunnen communiceren
10.	<u>Log & logging</u>	Het automatisch bijhouden van systeemveranderingen
11.	<u>SIEM</u>	Security Information Event Management: Geavanceerd algoritme wat netwerkverkeer analyseert om verdacht verkeer te detecteren
12.	<u>Load Balancing</u>	Het verdelen van het netwerkverkeer om zo overbelasting te voorkomen
13.	<u>Datalek</u>	Wanneer gevoelige data openbaar komt te staan
14.	<u>NCSC</u>	Nationaal Cyber Security Centrum; Een groep IT-specialisten welke helpen bij het afhandelen van beveiligingsincidenten
15.	<u>CERT</u>	Computer Emergency Response Team; Een interne groep IT-specialisten voor het afhandelen van beveiligingsincidenten
16.	<u>Forensisch onderzoek</u>	Het grondig analyseren van (gecomprimeerde) systemen en bestanden
17.	<u>IT</u>	Information Technology; Informatietechnologie, alle hard- & software die iets doen met digitale gegevens.
18.	<u>OT</u>	Operational Technology; Operationele technologie, alle hard- & software welke fysieke taken verrichten.
19.	<u>RTO</u>	Recovery Time Objective; Wanneer welke systemen weer operationeel moeten zijn in het geval van een incident
20.	<u>RPO</u>	Recovery Point Objective; Welke systemen/ data het belangrijkste zijn om niet gecompriemerd te raken
21.	<u>CPU</u>	Central Processing Unit; Het computeronderdeel welke taken uitvoert
22.	<u>RAM</u>	Random Access Memory; Het computeronderdeel welke taken bijhoudt wat de CPU moet uitvoeren
23.	<u>Backdoor</u>	Een manier voor derden om ongeautoriseerd toegang te krijgen in het netwerk
24.	<u>Snapshot</u>	Een uitgebreide back-up welke ook gedetailleerde informatie bevat over het systeem op het moment zelf
25.	<u>Ransomware</u>	Malware welke zo veel mogelijk bestanden encryptie en meestal vraagt naar losgeld voor de encryptie bestanden
26.	<u>Keylogger</u>	Malware wat de toetsen die worden ingedrukt opslaat in mogelijke verstuurt naar externe partijen om zo bv. inloggegevens te krijgen

27.	<u>Screening</u>	Het onderzoeken & analyseren van de achtergrondinformatie van een (toekomstige) medewerker.
28.	<u>GIS</u>	Geografische informatiesysteem; Beheer, analyseren en visualiseren van geografische gegevens
29.	<u>EMS</u>	Energy Management System; Beheer van elektriciteitsproductie, - distributie, -transmissie, inclusief real-time monitoring, controle en optimalisatie van energiebronnen en -netwerken
30.	<u>CRM</u>	Customer Relationships Management; Softwaresysteem waarin klantgegevens en relaties worden opgeslagen.
31.	<u>ERP</u>	Enterprise Resource Planning is software voor het integraal beheren van bedrijfsprocessen zoals financiën en voorraadbeheer.

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.

Dit document volgt de SANS framework zoals beschreven in *The Guide to Cyber Incident Response Planning* (FOX IT, 2021). Er is voor deze framework gekozen want deze beschrijft een completere en gedetailleerde DRP dan NIST. In het document komen dan ook de 6 stappen terug van SANS: Preperation, Identification, Containment, Eradication, Recovery en Lessons learned.

Het is van cruciaal belang dat dit plan regelmatig wordt getest en verder wordt afgestemd. Het niet navolgen en verbeteren van dit plan kan resulteren in 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 DRP regelmatig te testen en af te stemmen heeft meerdere belangrijke voordelen, ten eerste zijn de Incident Response Teams (IRT) 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 DRP. Hierdoor zijn de IRT's nog beter voorbereid voor een echt security incident.

2. Inventarisatie

In dit hoofdstuk zal er beschreven en toegelicht worden wat de IT&OT inhoudt binnen Winfra Vital. Er zal dus een inventarisatie worden uitgevoerd om dit te bepalen.

2.1. IT

Nr.	Naam	Toelichting
1.	ERP	Software wat kantoorautomatisering verzorgt.
2.	Firewall/routers	Firewalls blokkeren bepaalde IP-adressen en poorten, en routers reguleren het bestaande netwerk/creëren een nieuw netwerk.
3.	Antivirus	Analyseert en detecteert malware en verwijdert deze vervolgens.
4.	GIS	Analyseert geografische gegevens om duidelijk te krijgen waar verkeer naar toe moet.
5.	EMS	Behandelt verkeer van stroom.
6.	CRM	Dit systeem bevat persoonsgegevens van klanten.
7.	Computers en tablets	Deze apparaten zijn gekoppeld aan het netwerk van Winfra Vital.

Tabel 1, IT-onderdelen Winfra Vital.

2.2. OT

Nr.	Naam	Toelichting
1.	Toegangspasjes	Met deze pasjes mogen asleen bepaalde personen/functies komen waar ze horen te komen.
2.	Toegangsscanners	Scannen de toegangspasjes en verlenen toegang tot locaties.
3.	Slimme meters	Staan in gebruikers hun huizen/gebouwen zodat ze niet handmatig meterstanden hoeven door te geven.
4.	Netwerk switches	Verlengen het bestaande netwerk door meer ethernetpoorten aan net bieden en/of wifi te versterken
5.	Servers	Hiermee wordt data opgeslagen en verstuurd.
6.	Schakelaars/relais	Deze schakelapparatuur wordt gebruikt om de stroomvoorziening te regelen.
7.	Transmissielijnen, gasleidingen	De lijnen die de elektriciteit en gas over lange afstanden transporteert vanaf de opweklocaties naar de distributienetwerken.
8.	Distributienetwerk	Dit netwerk levert elektriciteit en gas aan residentiële, commerciële en industriële klanten.
9.	Windparken	Parken waarop windmolens staan.
10.	Zonneparken	Parken waarop zonnepanelen staan.

Tabel 2, OT-onderdelen Winfra Vital.

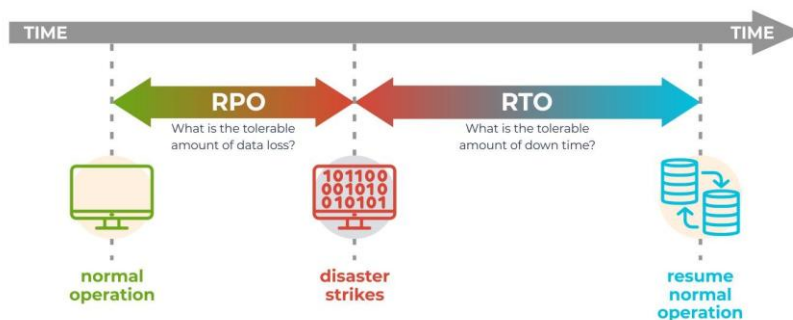
3. RPO & RTO

In dit hoofdstuk worden het RPO en RTO toegelicht. Er zal worden bepaald wat het RPO en RTO is. Ook zal er worden toegelicht waarom het belangrijk is om deze te behalen. In de tabel hieronder is een overzicht van de assets te zien welke onder het RPO vallen, met een prioriteit en een toegewezen RTO.

Asset	RPO	Prioriteit	RTO
Schakelaars/relais	Verdeelt het stroom verkeer	5	< 6 uur
Transmissielijnen, gasleidingen	Transporteren gas & stroom	5	< 6 uur
Distributienetwerk	Verdeelt gas & stroom verkeer	5	< 6 uur
GIS	Helpt verdelen vitaal verkeer	4	< 12 uur
EMS	Zorgt o.a. voor stroomvoorziening	4	< 12 uur
ERP	Zorgt ervoor dat medewerkers hun kantoortaken kunnen uitvoeren	3	< 24 uur
Computers en tablets	Zorgt ervoor dat medewerkers hun kantoortaken kunnen uitvoeren	3	< 24 uur
Servers	Bevat persoonsgegevens & reguleert dataverkeer	3	< 24 uur
Firewall/routers	Zorgt voor netwerk	2	< 48 uur
Antivirus	Voorkomt verspreiding malware	2	< 48 uur
Netwerk switches	Verdelen het netwerk	2	< 48 uur
CRM	Bevat persoonsgegevens, mag niet gelekt worden	1	< 72 uur
Slimme meters	Kan voor imago schade zorgen	1	< 72 uur

Tabel 3, RPO & RTO tabel voor verschillende assets.

De belangrijkste functionaliteit voor Winfra Vital is de stroom & gas voorziening. De assets die hiermee direct te maken hebben krijgen de hoogste prioriteit en zijn dus de belangrijkste RPO's. We hebben besloten om prioriteit als score mee te geven om zo duidelijk aan te tonen wat de belangrijkste RPO's zijn. De RTO's zijn direct verbonden aan de prioriteiten score.



Figuur 1, RPO & RTO.

4. Preparation

4.1. Policy

1. Zorg voor dagelijkse back-ups naar online back-up systemen.
2. Eens in de maand moeten de online back-ups nog een keer geback-upt worden naar offline back-ups.
3. Ook moet dan worden gecontroleerd of de back-ups terug te zetten zijn.
4. De back-ups moeten minimaal een half jaar teruggaan.
5. Zorg voor bewustwordingstraining voor het personeel.
6. Meet ook het bewustwordingen niveau door de training regelmatig uit te voeren en met oefeningen.
7. Zorg ervoor dat het personeel gescreend wordt voordat ze worden aangenomen. Om zo te controleren of ze niet chanteerbaar zijn en/of een inside threat kunnen vormen.
8. Implementeer een vier-ogen principe.
9. Implementeer de Role Based Access Control voor de accounts.
10. Houd een lijst bij van wie toegang heeft tot welk account.
11. Elk account moet met 2-staps verificatie beveiligd worden.
12. De wachtwoorden moeten minimaal 16 tekens lang zijn.
13. Zorg dat elk systeem de laatste beveiligingsupdates hebben.
14. Maak gebruik van firewalls en antivirussen.
15. Implementeer segmentatie architecturen voor het netwerk.
16. Voer om het jaar een pentest uit.
17. Houd een lijst bij met alle hardware en software en update deze lijst wekelijks.
18. Implementeer load balancing in het netwerk om zo beter bestemt te zijn tegen DDoS aanvallen.
19. Alles wat er in het systeem gebeurt wordt gelogd.
20. Van de logging worden back-ups gemaakt.
21. Het systeem mag alleen logs toevoegen. De logs mogen niet worden aangepast.
22. Implementeer een goed voorgetrained SIEM omgeving.
23. Zorg ervoor dat een test omgeving geen data en toegang bevat/heeft tot de productie omgeving en vice versa.

4.2. Response plan/strategy

Incident	Impact	Urgentie	Score	Beschrijving
Malware	5	5	25	Malware heeft de potentie om alles plat te leggen intern en het onherstelbaar te maken. Ook kan dit lastig te detecteren zijn, wat het een nog grotere bedreiging maakt.
Inside threat	5	5	25	Een inside threat heeft de potentie om alles plat te leggen intern en het onherstelbaar te maken zowel online als offline. Ook kan dit lastig te detecteren zijn, wat het een nog grotere bedreiging maakt.
DDoS	4	5	20	Een DDoS aanval is relatief makkelijk te bestrijden. Ook valt dit meestal niet meteen je hele systeem aan maar richt het zich op een gedeelte. Dit hangt natuurlijk wel van af welk systeem een doelwit is.
Datalek	4	4	16	Voor een vitale aanbieder is een datalek minder cruciaal want het verwerkt geen bijzondere persoonsgegevens. Wel kunnen er belangrijke account inlog gegevens gelekt worden.
Phishing	3	3	9	De meeste phishing is een random mail die iemand krijgt van een geautomatiseerd systeem. Het is dus niet direct gericht op het bedrijf zelf en heeft dan ook waarschijnlijk weinig impact. Bij sprake van spearphishing ligt dit natuurlijk anders. Daarom is het cruciaal om toch hiervoor belangrijke maatregel te hebben.

Tabel 4, Impact x Urgentie van incidenten.

4.3. Communication

1. Omdat Winfra een vitale aanbieder is, zijn zij verplicht om nauw samen te werken met de NCSC. Dit houdt in regelmatige rapportage, delen van relevante informatie en het aannemen van aanbevelingen.
2. Elk incident moet direct worden gemeld bij de NCSC, ook wanneer het incident verholpen is.
3. Melding bij het NSCS moet plaatsvinden via de gespecificeerde vastgestelde kanalen.
4. In geval van grootte incidenten verloopt de externe communicatie via een getrainde woordvoerder van Winfra vital deze vermeld updates via officiële kanalen, zoals persberichten of de website van Winfra vital.
5. Er wordt rekening gehouden met een need-to-know policy, waardoor gevoelige/vertrouwelijke informatie alleen gedeeld wordt de betreffende personen.
6. Naast externe communicatie worden er communicatieprotocollen vastgesteld voor het informeren van interne partijen, zoals het managementteam, IT-personeel en anderen betrokkenen.
7. Voor zowel interne als externe communicatie worden er duidelijk richtlijnen vastgesteld om een gecoördineerde respons te garanderen.

4.4. Documentation

1. Elke stap die het NCSC en CERT neemt wordt gedetailleerd bijgehouden en gedocumenteerd
2. Hierin moet worden bijgehouden voor elke actie de wie, wat, waar, wanneer, hoe en waarom voor het uitvoeren hiervan.

4.5. Team

1. Het NCSC en CERT moet bestaan uit diverse experts om zo goed mogelijk voorbereid te zijn voor verschillende scenario's het CERT-team staat beschreven in het CERT-document.
2. Er moet duidelijk beschreven staan wie waarvoor verantwoordelijk is tijdens een incident.
3. Bij incidenten met de hoogste urgentie (urgentie 5) geldt de huidige hiërarchie niet meer, de CERT & NCSC hebben dan de hoogste rang.
4. De teams moeten toegang krijgen tot de benodigde IT-middelen om het incident zo snel en effectief mogelijk aan te pakken.

4.6. Tooling

In het geval van een security incident moet het CSIRT onmiddellijk toegang krijgen tot de volgende middelen:

1. De verschillende geïmplementeerde monitoring en logging systemen
2. Malware: Back-up systemen en het mogelijke herstel hiervan
3. Desbetreffende communicatie middelen/kanalen
4. Volledige toegang tot de verschillende netwerk en internetsystemen
5. DDoS: Analyse tools voor het uitzoeken van waar de DDoS plaatsvindt
6. DDoS: De mogelijkheid om het internet uit te schakelen mocht het van buitenaf komen

7. Phishing: De mogelijkheid om de mail te controleren en forensisch onderzoek op de link uit te voeren
8. Inside Threat: Mogelijkheid om account van desbetreffende entiteit te termineren.

4.7. Training

1. Het personeel verantwoordelijk voor de IT-beveiliging moet jaarlijks worden bijgeschoold.
2. Verschillende security incidenten worden jaarlijks geoefend.
3. Dit geldt ook voor de verschillende partijen verantwoordelijk voor de communicatie, zoals publieke relaties en de toegewezen woordvoerder.

5. Identification

Het detecteren en identificeren van een incident is de tweede stap. Er kan pas efficiënt te werk worden gegaan als het bekend is policwat het incident is. Het analyseren van deze incidenten moet door minimaal twee mensen worden uitgevoerd; Een om het te identificeren en te onderzoeken, en een om bewijs te verzamelen.

Mogelijke afwijkingen kunnen zijn:

1. Onaangekondigde verandering van accounts rechten
2. Onaangekondigde toevoeging van een account
3. Een nieuwe login van een account op een andere locatie
4. Verdacht gedrag bij een account
5. Mislukte inlog pogingen
6. Meldingen en/of waarschuwing van firewall en/of antivirus systemen
7. Een verandering van belangrijke bestanden, zoals nieuwe opstart services, wachtwoord locaties, configuratie bestanden en webserver folders
8. Nieuw plotseling verschenen software
9. Onverwacht gebruik van een netwerkpoort
10. Nieuwe verbinding van onbekend apparaat
11. Verhoogd gebruik van computer en systemen bronnen, zoals CPU, RAM, Lezen/Schrijven en Downloaden/Uploaden
12. Mogelijk verdachte e-mails met links en/of bestanden erin

Wanneer een afwijking in de normale werking plaatsvindt en dit inderdaad wordt geclassificeerd als kwaadwillend, moet het CERT de bedreiging onmiddellijk aanpakken en proberen op te opsluiten.

6. Containment

6.1. Malware

In het geval van een Malware aanval moeten de geïnfecteerde systemen zo snel mogelijk afgezonderd worden van de rest. Dit kan gedaan worden door bijvoorbeeld de systemen uit te zetten of toegang tot het netwerk te verbieden. Dit kan worden gedaan door bijvoorbeeld de kabels eruit te trekken.

Van de geïnfecteerde systemen moet ook een back-up worden gemaakt, om forensisch onderzoek te kunnen uitvoeren. Op deze manier kan er worden nagegaan wat er precies misging en via welke weg ze geïnfecteerd geraakt konden worden.

Hierna moet worden geïdentificeerd welke systemen er zijn geïnfecteerd en of de normale werking opgebouwd kan worden. Dit kan bijvoorbeeld door de geïnfecteerde systemen te wissen en dan de oude back-ups erop te zetten, of door de niet geïnfecteerde systemen te herconfigureren.

6.2. DDoS

In het geval van een DDoS aanval kan simpelweg de IP-adressen geblokkeerd worden van waar de aanval plaatsvindt. Ook kan de DDoS omgeleid worden naar een ongebruikt systeem om zo de belangrijke systemen niet te overbelasten.

6.3. Phishing

Bij melding van phishing moet het mogelijk gecompromiteerde systeem direct afgezonderd worden van het netwerk. Ook moet het account (tijdelijk) geblokkeerd worden.

6.4. Inside Threat

Account van desbetreffende entiteit moet direct bevroren worden. Om zo later te kunnen controleren hoe en waar het account gebruik van gemaakt heeft. Ook moet het direct uitgelogd worden overal.

7. Eradication

Voordat de malware en incident verwijderd wordt, moet hiervoor eerst een snapshot gemaakt worden van de betreffende systemen en diensten, om zo niet de sporen te wissen van hoe het incident het kunnen plaatsvinden.

Bij elke vorm van incident behoort altijd gecontroleerd te worden op mogelijk nieuwe backdoors, accounts, en andere artefacten die aangemaakt kunnen worden tijdens een incident. Deze behoren ook grondig te worden verwijderd nadat er een goede snapshot in gemaakt van alle logs en de stand van het huidige systeem. Hierdoor kunnen de systemen worden hersteld en kan worden achterhaald wat we hiervan kunnen leren, wat erg belangrijk is en terugkomt in de laatste fase.

7.1. Malware

7.1.1. Ransomware: Betalen van losgeld

Mocht de waarde van het losgeld minder zijn dan de kosten voor het zelfstandig verwijderen en mogelijke vervangen van de systemen, dan is het verstandig om het losgeld te betalen. Zo bespaar je tijd en geld en kan de normale gang van zaken worden hervat. Dit is al helemaal handig voor wanneer ook de back-ups zijn geïnfecteerd.

7.1.2. Zelf regelen

Wanneer het losgeld te hoog wordt geacht, de kans op volledig herstel te laag is, en/of de tijd van herstel niet te lang duurt kan er gekozen worden om zelf de systemen te herstellen.

Deze stap verschilt per soort malware en hoeveel systemen/bestanden geïnfecteerd zijn geraakt. Wanneer bijvoorbeeld de malware de gehele opslag van een computer heeft geëncrypt, is het handig om deze opslag in zijn geheel te vervangen, een oude back-up terug te zetten en dan de mogelijke noodzakelijke stappen zetten om alles weer up-to-date te krijgen.

7.2. DDoS

Voor een DDoS aanval van buiten is het beste om het verkeer te blijven omleiden naar een ongebruikt gedeelte van het netwerk.

Bij een aanval binnenin moeten de systemen van waar de aanval plaatsvindt gelokaliseerd worden en van het netwerk verwijderd worden. Hierin moet dan de malware verwijderd worden welke de aanval uitvoert waarna de systemen weer up-to-date gebracht moeten worden.

7.3. Phishing

Om de artefacten van phishing te verwijderen verschilt de aanpak per soort phishing. Met phishing kan bijvoorbeeld een legitiem uitziende website jouw inloggegevens of dergelijke keyloggen. Ook kan de link en/of bestand malware installeren op het systeem zelf. Het is belangrijk om de mail niet te verwijderen, maar juist een copy hiervan te maken om het later te onderzoeken.

In het geval van geïnstalleerde malware moeten de hierboven genoemde maatregelen uitgevoerd worden. Bij datalek van bijvoorbeeld accountgegevens moeten de gecompriemde accounts geblokkeerd worden.

7.4. Inside Threat

Analyseer, lokaliseer en verwijder de door de inside threat's account gemaakte artefacten.

8. Recovery

8.1. Malware

Wanneer het NCSC zeker van lijkt te zijn dat de aanval gestopt en verwijderd is, kan het herstelproces beginnen. Aan de hand van de ernst van de aanval kan er gekozen worden om de back-up terug te zetten, of het hele systeem her-instellen. Na het herstel is het ook verstandig om extra beveiligingsmaatregelen te implementeren in het systeem.

Na het herstel hiervan moet zorgvuldig gemonitord worden of de aanval nu niet alsnog terugkomt, hoelang deze stap duurt verschilt per incident en de aard van de malware. Een malware wat pas geactiveerd wordt na een maand is bijvoorbeeld lastiger te monitoren dan degene die meteen aanvalt.

8.2. DDoS

Wanneer de malware verwijderd is van de interne systemen moet ook goed gecontroleerd worden of de malware inderdaad goed verwijderd is na herstel. Deze stap is identiek met de vorige. Mocht het een aanval van buitenaf zijn welke gestopt lijkt te zijn, kunnen de IP-adressen gedeblokkeerd worden en/of hun netwerkverkeer weer de normale route laten volgen.

8.3. Phishing

Bij een gecompromeerd systeem met malware moeten dezelfde maatregelen genomen worden als hierboven vermeld. Bij gecompromeerde accounts moet het wachtwoord gereset worden en overal worden uitgelogd.

8.4. Inside Threat

Maak kopie van account en reset het wachtwoord van het account.

9. Lessons Learned

Nadat alle systemen zijn hersteld en de normale gang van zaken zijn hervat, is het cruciaal om de volgende stappen uit te voeren, om zo het plaatsgevonden incident te voorkomen voor de volgende keer:

1. Verzamel alle bewijsmateriaal en documentatie over het plaatsgevonden incident.
2. Maak hiervan een gedetailleerd rapport waarin de mogelijke wie, waar, wat, wanneer, waarom en hoe vragen over het incident beantwoord staan.
3. Voer vervolgens een meeting uit waarin alle partijen die te maken hadden met het incident aanwezig zijn en het rapport wordt gepresenteerd en verder uitgewerkt.
4. Tijdens de meeting komen dan benodigde verbeteringen en geleerde lessen uit.
5. Wanneer het rapport is afgewerkt en alle mogelijke verbeteringen zijn verzameld moet dit gepresenteerd worden met de relevante stakeholders van de organisatie.
6. Het is dan cruciaal dat deze verbeterpunten zo snel mogelijk worden doorgevoerd om zo zo'n incident te voorkomen in de toekomst.

Bibliografie

FOX IT. (2021). *The Guide to Cyber Incident Response Planning*. Retrieved from Fox IT:
https://www.fox-it.com/media/4xrla5rm/ncc-group_-the-guide-to-incident-response-planning.pdf