Incident response en recovery

www.securitydelta.nl/ipcs

IPCS
INDUSTRIEEL
PLATFORM
CYBER SECURITY

Revisie

datum	naam	revisie
10-apr-2025	Johan Assies	Eerste IPCS (HSD) uitgave 2025Q2, NIS2 bijgewerkt.
11-apr-2025	Marcel Jutte	QC en contactinformatie geactualiseerd

1. Incident response en recovery

Bedrijven nemen veel maatregelen om zich te beschermen tegen cyberaanvallen. Hackers kunnen zich toegang verschaffen tot een netwerk met als doel data te stelen of te vergrendelen middels ransomware, vaak voor financieel gewin.

Ondanks de genomen maatregelen is het niet uit te sluiten dat een bedrijf op enig moment tóch getroffen worden door een cyberaanval. Een snelle en adequate reactie helpt om de schade zoveel mogelijk te beperken. Maar snel reageren kan alleen als hier vooraf al goed over nagedacht is: wie, wat, waarmee, wanneer. Dit document is bedoeld om bedrijven te helpen zich hierop voor te bereiden.

2. Wat is een cyberincident?

Het Nationaal Cyber Security Centrum (NSCS) definieert een cyberincident als: “Een inbreuk op het beveiligingsbeleid van een systeem, om de integriteit of beschikbaarheid ervan aan te tasten, en/of de ongeoorloofde (poging tot) toegang tot een systeem of systemen.”

Enkele voorbeelden van inbreuken:

1. Pogingen om onbevoegd toegang te krijgen tot een systeem en/of gegevens.
2. Het ongeoorloofd gebruik van systemen voor het verwerken of opslaan van gegevens.
3. Wijzigingen in de firmware, software of hardware van een systeem zonder toestemming van de systeemeigenaar.
4. Kwaadwillige verstoring of beïnvloeding van de juiste werking (“denial of service”).

3. Inregelen organisatie

Als er een cyberincident is, dan moet snel gehandeld worden. Er is geen tijd om na te gaan denken over wie wat moet doen. Hoe sneller de reactie op het incident, des te lager de schade zal zijn.

In een organisatie zijn vaak al overleg- of crisisstructuren aanwezig om te reageren bij een veiligheidsincident, zoals een brand of een ongeval. Neem dit als voorbeeld om een structuur voor een cyberincident op te stellen:

1. Bepaal hoe crisisteams eruit komen te zien;
2. Bepaal welke taken het crisisteam moet oppakken;
3. Bepaal escalatiepaden naar hogere crisisteams (afhankelijk van de grootte en volwassenheid van de organisatie);
4. Bepaal welke taak door welke functionaris wordt uitgevoerd.

Na detectie van een cyberincident is het eerste doel om deze zo snel mogelijk te isoleren, zodat verdere verspreiding voorkomen wordt is. Vervolgens moet bepaald worden of het systeem geïsoleerd

moet blijven voor forensisch onderzoek. Is dat het geval, dan moet recovery op een andere resource plaatsvinden. Is forensisch onderzoek niet nodig, dan volgt de recovery fase: terugbrengen van de systemen in operationele staat.

4. Crisisteam – taken en verantwoordelijkheden

Het crisisteam is verantwoordelijk voor een gestructureerde aanpak van zowel de incident response als de incident recovery (hieronder in meer detail besproken).

Een andere belangrijke taak is het verzorgen van de communicatie. Vooraf moet een communicatieplan opgesteld worden waarin vermeld staat wie op welk moment geïnformeerd wordt en wie er communiceert. Denk hierbij aan (onder andere):

- Directie / management.
- Medewerkers.
  Bijvoorbeeld: is het nodig om opkomende ploegen te informeren dat ze tijdelijk niet hoeven te komen werken, of dat PC's niet aangezet mogen worden, en waarom thuiswerkers niet kunnen inloggen.
- Leveranciers en klanten.
  Bijvoorbeeld: om afspraken te maken over het tijdelijk stopzetten van leveringen om verkeersinfarcten op de locatie te voorkomen. Als er geen vrachtwagens in- en uitgeladen kunnen worden, moeten deze vrachtwagens van het terrein geweerd worden.
- Overheidsinstanties.
  Bijvoorbeeld: als er een mogelijk gevaar bestaat voor de omgeving, bijvoorbeeld vanwege een lozing van gevaarlijke stoffen, of door 'loss of control' van procesinstallaties. Als er een incident met aanzienlijke gevolgen voor de continuïteit van de geleverde dienst van een vitale aanbieder optreedt, dan is ook een melding vereist (NCSC in het kader van de WBNI).
- Opsporingsinstanties.
  Bijvoorbeeld: politie, als er sprake is van criminele activiteiten zoals hacking / ransomware.
- Systeem integratoren, hardware-leveranciers, cybersecurityspecialisten.
  Bijvoorbeeld: om af te stemmen waar en wanneer externe hulp benodigd is, of snel nieuwe apparatuur geleverd moet worden.

De communicatieafdeling zal betrokken moeten worden indien externe communicatie (bijvoorbeeld: pers) nodig is. Voorbeelden uit het verleden leren dat een open communicatie over een groot cyberincident, en de consequenties daarvan, positief worden opgevat.

Communicatie met medewerkers kan het beste verlopen via onafhankelijke media die op een smartphone te installeren zijn (bijvoorbeeld Signal of WhatsApp, mits het interne beleid het gebruik van dit medium toestaat). De bedrijfsemail of eigen softwarepakketten kunnen mogelijk niet (meer) operationeel zijn.

5. Incident response plan

Het incident response plan beschrijft alle activiteiten die te maken hebben met het acteren op een incident. In het plan is het gehele proces van incident detectie t/m rapportage vooraf vastgelegd.

De volgende stappen kunnen deel uit maken van het incident response plan:

1. **Detectie van een incident**
2. **Rapportage van het incident**
3. **Eerste analyse**
4. **Insluiting van de dreiging**
5. **Controle over het incident**
6. **Overdracht aan het recovery team**
7. **Rapportage en evaluatie**

De uitvoering van deze stappen hoeft niet noodzakelijk in deze volgorde; mogelijk kunnen bepaalde stappen ook parallel uitgevoerd worden.

1. Detectie van een incident

Bepaal wanneer er sprake is van een incident en hoe dit opgemerkt kan worden. Cyberincidenten kunnen ook door personeel, of zelfs externen, gemeld worden. Er zijn legio voorbeelden van bedrijven die door leveranciers geattendeerd worden op afwijkingen (bijv. verdachte e-mails) waardoor een cyberincident ontdekt werd.

Ransomware is makkelijk te herkennen doordat bestanden versleuteld zijn en/of medewerkers een pop-up te zien krijgen met de melding dat hun bestanden gegijzeld zijn. Dat is echter te laat om preventief in te grijpen, beter is het om ransomware te detecteren voordat bestanden versleuteld worden.

Er zijn echter ook andere indicatoren die kunnen duiden op een incident, zoals afwijkend gedrag (anomalieën). Ook zijn er systemen (zoals een IDS – Intrusion Detection System) die kunnen informeren als er afwijkend gedrag wordt gedetecteerd. Het is belangrijk te realiseren dat de complexere cyberaanvallen zich kunnen manifesteren als operationele problemen.

2. Rapportage van incident

Bepaal aan wie incidenten worden gerapporteerd en zorg ervoor dat vastgelegd is welke incidenten zijn opgetreden. Hierbij dient ook aandacht besteedt te worden aan de correlatie die incidenten met elkaar kunnen hebben. Naarmate de ernst van een incident toeneemt moet nagedacht worden hoe breed er gecommuniceerd gaat worden, zowel in- en extern, door de verantwoordelijke personen.

3. Eerste analyse van het incident of de dreiging en eventuele opschaling

Bepaal de omgang van het incident: is het net aan de gang, of ziet het er naar uit dat het al langere tijd gaande is. Onderzoek ook de impact van het incident of de dreiging: is het beperkt tot een klein deel van de organisatie, of heeft het een grote invloed op (het functioneren van) de gehele organisatie.

Bepaal daarna of het incident gemeld moet worden aan de interne incident response organisatie (zoals bijv. crisisteam). Overleg ook of er externe ondersteuning nodig of dat het incident intern afgehandeld kan worden.

Op verschillende vlakken zijn er tegenwoordig wettelijke verplichtingen voor het melden van incidenten met als mogelijke oorzaak cyberincidenten. De eerste meldplicht komt voort uit de bescherming van persoonsgegevens als gevolg van datalekken. Daarnaast is een meldplicht voor bedrijven welke nu onder de Wbni[1], als uitvloeisel van de NIS[2] richtlijn, vallen. Dit zijn momenteel alle nationale kritische infrastructuren.

De NIS2 is eind 2022 vastgesteld door de Europese Unie. Daarna hebben de lidstaten nog tot 17 oktober 2024 om de NIS 2 landelijk door te voeren. Deze zal naar alle waarschijnlijkheid een meldplicht introduceren voor vrijwel alle productiebedrijven. Een aantal landen, waaronder Nederland heeft deze deadline niet gehaald. Naar verwachting wordt de NIS2 in Nederland in de tweede helft van 2025 actief. Deze zal dan de Cyberbeveiligingswet (Cbw) gaan heten.

4. Insluiten van de bedreiging

Bepaal hoe de dreiging ingesloten kan worden zodat het zich niet verder over de organisatie kan verspreiden, houdt hierbij rekening met Cloud omgevingen en medewerkers die remote of op andere locaties werken.

Denk hierbij aan het afsluiten van netwerksegmenten, uitschakelen van routers en switches of het compleet afsluiten van locaties, afschakelen van PC's, waarschuwen van medewerkers om PC's / laptops juist niet aan te zetten, etc.

Aangezien het afsluiten van systemen het herstel en/of forensisch onderzoek kan bemoeilijken, moet duidelijk zijn wat tot de minste schade leidt: het uitschakelen van systemen, of het juist ingeschakeld laten hiervan. Forensisch onderzoek kan in eerste instantie tot hogere kosten leiden, doordat systemen langere tijd niet beschikbaar zijn, het kan echter wel helpen in het voorkomen van toekomstige incidenten.

[1] Wbni: Wet Beveiliging Netwerk en Informatiesystemen; Nederlandse uitwerking van de NIS richtlijn.

[2] NIS: Netwerk en Informatiesystemen, richtlijn van de Europese Commissie

5. Controle over het incident

Het is belangrijk het incident onder controle te krijgen. Dit houdt in dat: de dreiging gestopt is, dat de gaten gedicht zijn, en dat zeker gesteld is dat de aanvallers/malware niet meer in de systemen actief zijn, of weer actief kunnen worden.

Controle van incidenten is direct gerelateerd aan de detectiefase. Het is belangrijk tijdens de controlefase alle beschikbare detectiemethodieken te blijven gebruiken.

6. Overdracht aan recovery team

Nadat het incident onder controle gebracht is, kan het overgedragen worden aan het recovery team. Zij gaan aan de slag (zie “Incident recovery plan”) om de getroffen netwerken en systemen te herstellen naar de normale operationele staat.

7. Rapportage en evaluatie

Na afloop wordt er een rapportage opgesteld over het incident. Deze rapportage beschrijft onder andere hoe het incident heeft kunnen gebeuren en hoe de afhandeling van het incident verlopen is. Tevens wordt er een evaluatie gehouden waarin besproken wordt hoe de verschillende fasen zijn verlopen en welke lessen hieruit geleerd kunnen worden.

6. Incident recovery plan

Het incident recovery plan beschrijft alle activiteiten die te maken hebben met het herstellen van de systemen naar de normale operationele staat. Onderstaande stappen kunnen deel hier deel van uit maken:

1. **Prioritering systemen**
2. **Terugzetten back-ups**
3. **Herconfigureren apparatuur**
4. **Vervanging apparatuur**
5. **Controleren en testen**
6. **Inbedrijfstellen**
7. **Bijwerken CMDB**
8. **Nieuwe back-ups maken**
9. **Rapportage en evaluatie**

1. Leg vast welke systemen het eerste weer beschikbaar moeten zijn.

Dit hangt af van welke systemen getroffen zijn, maar kan ook afhankelijk zijn van de aanwezige voorraad, planning, verkopen etc. De opstarttijd van systemen kan ook van invloed zijn; systemen met een lange opstarttijd kunnen misschien beter als eerste worden hersteld.

Een productielijn waarbij een product gefabriceerd wordt waar weinig voorraad van is maar waar wel een hoge vraag naar is, zal eerder hersteld moeten worden dan een productielijn waarbij nog veel voorraad aanwezig en er een geringe vraag is. Ook aspecten als houdbaarheid van halffabricaten of eindproducten kunnen een rol spelen.

2. Terugzetten van back-ups

In een aantal gevallen kunnen systemen hersteld worden door het terugzetten van back-ups. Deze systemen moeten echter goed gecontroleerd zijn voordat ze opnieuw met het netwerk worden verbonden. Dit om er zeker van te zijn dat er geen vroege versies van eventuele malware of ransomware (aanwezig in de back-up) mee teruggezet is. Overweeg tevens of het mogelijk is de recovery op geïsoleerde systemen uit te voeren.

Let op dat back-up software wel moet kunnen werken als delen van de infrastructuur mogelijk afgeschakeld zijn, zoals file servers, netwerkinfrastructuur, of AD (Active Directory) servers.

3. Herconfigureren van apparatuur

Het kan zijn dat apparatuur opnieuw geconfigureerd moet worden omdat er instellingen gewijzigd zijn. Ook kan het zijn dat systemen opnieuw geïnstalleerd moeten worden.

Zorg ervoor dat van alle (belangrijke) systemen documentatie beschikbaar is. In deze documentatie moeten belangrijke parameters en eventuele installatie instructies beschreven worden. Houd er rekening mee dat deze documentatie zo opgeslagen wordt dat ze altijd beschikbaar zijn. Dit kan door de documentatie online (bijv. clouddienst) op te slaan of door ze uit te printen en in ordners op te slaan (zorg er dan wel voor dat deze brandveilig worden opgeborgen!

4. Vervanging van defecte apparatuur

Het kan zijn dat apparatuur (zoals computers) dermate beschadigd zijn dat ze vervangen moeten worden. Ook kan het verstandig zijn, met het oog op het voorkomen van nieuwe besmettingen, om getroffen apparatuur niet meer in te zetten. In dat geval zullen tientallen of wellicht honderden nieuwe systemen gekocht en ingericht moeten worden.

Van tevoren moet al nagedacht worden over welke leverancier(s) welk percentage van de benodigde hoeveelheid systemen kan/kunnen leveren, en welke (externe) hulp er ingeschakeld kan worden om de nieuwe systemen in te richten.

5. Controle / testen van alle vervangen/ betrokken systemen

Alle systemen die betrokken zijn bij het incident moeten gecontroleerd worden om zeker te zijn dat ze weer goed functioneren. Bij productiesystemen kan het zelfs aan te bevelen zijn hiervoor FAT en SAT procedures toe te passen.

6. In bedrijf stellen van de systemen

Nadat alle systemen gecontroleerd en getest zijn, kunnen ze weer in bedrijf genomen worden. Hierbij moet goed gemonitord worden of ze weer naar behoren functioneren en geen afwijkend gedrag vertonen.

7. CMDB Bijwerken

Alle (configuratie-)wijzigingen moeten verwerkt worden in het CMDB (Configuration Management Database), zodat deze actueel blijft.

8. Nieuwe back-ups maken

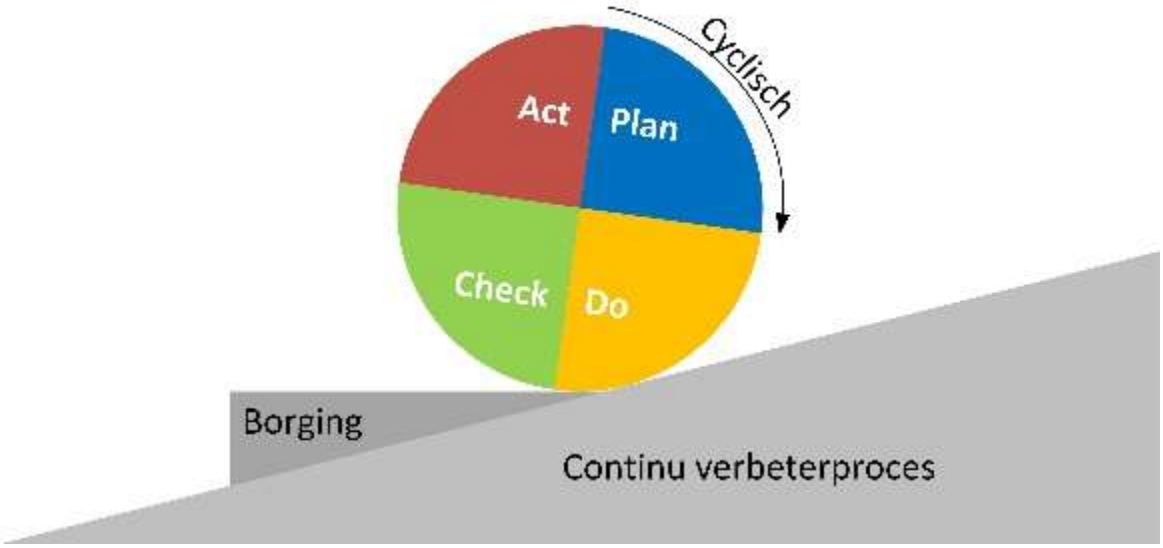
Van de systemen die opnieuw zijn opgebouwd/geïnstalleerd, moeten nieuwe back-ups gemaakt worden zodat bij nieuwe cyberincidenten weer goede (actuele) back-ups beschikbaar zijn. Bij het inzetten van nieuwe apparatuur is een back-up net vóór ingebruikname van belang.

9. Rapportage en evaluatie

Na afloop van de incident recovery fase moet vastgelegd worden welke stappen zijn uitgevoerd en moet besproken worden wat er goed ging, en wat verbeterd moet/kan worden. Aan de hand hiervan kunnen de incident response en recovery plannen herzien worden.

7. PDCA – Plan, Do, Check, Act

Aan de hand van de PDCA cyclus moeten de incident detectie- en incident recovery plannen regelmatig doorgenomen worden. Hiermee is te voorkomen dat eventueel gewijzigde situaties (apparatuur, netwerken, organisatiestructuur, personen) niet in de plannen meegenomen worden.



Deze publicatie kunt u opvragen via ipcs@securitydelta.nl

Meer info over IPCS via https://securitydelta.nl/ipcs

Dit document is opgesteld door de volgende leden van het Industrieel Platform Cyber Security:

Johan Assies, Eric ten Bos, Michael Theuerzeit.

Met dank aan Rob Hulsebos voor het redigeren van de teksten, en de overige leden van de 'IPCS werkgroep IEC 62443' voor het reviewen van dit document.

Security Delta (HSD)
Wilhelmina van Pruisenweg 104
2595 AN The Hague
070 204 41 80

info@securitydelta.nl
www.securitydelta.nl