STAPPENPLAN
Hoe te handelen na een cyberincident

Wat moet er gebeuren in de eerste paar minuten na het constateren van een (potentiële) cyberaanval? En welke stappen moet het IT-team zo snel mogelijk ondernemen? In dit stappenplan lees je kort en bondig wie wat wanneer moet doen, om de schade zo beperkt mogelijk te houden.

Pro-tip: gebruik dit stappenplan als inspiratie of als basis voor het opstellen van een eigen stappenplan. Pluspunten voor het ontwikkelen van een eigen stappenplan voor eindgebruikers in een stijl en met taalgebruik die zij begrijpen.

Disclaimer: dit is geen incident response plan. In een incident response plan staan alle procedures – diep tot in de enen en nullen 😲 – uitgebreid beschreven die moeten worden opgevolgd als er een incident plaatsvindt, om zo gecoördineerd actie te ondernemen. Het document dat je nu bekijkt is een quicklist: een eerste stappenplan om te handelen na een cyberincident.

1

STAP 1 – VERBREEK DIRECT DE NETWERKVERBINDING

Ontdek jij als werknemer ongewone activiteiten aan je computer of laptop of klik je per abuis op een phishingmail? Verbreek dan direct de netwerkverbinding(en).

Om het apparaat direct los te koppelen van het netwerk kan de netwerkkabel losgetrokken worden en/of de Wi-Fi uitgeschakeld worden. Dit kan eventueel met (telefonische) hulp van een IT- of servicedeskmedewerker. Maar wacht zeker niet te lang. Haast en spoed is in dit geval goed. 😉

Let op: schakel niet het systeem uit, maar verbreek alleen de netwerkverbinding. Als het systeem uitgezet wordt, zullen eventuele sporen van het incident verloren gaan.

2

STAP 2 – MELD HET INCIDENT

Neem na het verbreken van de netwerkverbinding contact op met de IT-afdeling of de servicedesk om hen te informeren. Stel ook je leidinggevende op de hoogte.

Het geeft niet als later blijkt dat het een vals alarm is, maar als er iets vreemds aan de hand is, moeten de IT-medewerkers en de securityverantwoordelijke het weten. Soms voeren hackers of aanvallers hun acties onder de radar uit, zodat ze onopgemerkt toegang tot het (gehele) netwerk proberen te verkrijgen. Onregelmatigheden moeten altijd dus altijd gemeld en gerapporteerd worden.

3

STAP 3 – CONTROLEER OF DE NETWERKVERBINDING IS VERBROKEN

Controleer als eerste of de netwerkverbinding correct is verbroken.

Stel de volgende vragen aan de gebruiker – zo kun je de juiste vervolgstappen bepalen en het dreigingsniveau:

- ✔ Waar is het ontdekt?
- ✔ Wanneer is het ontdekt?
- ✔ Wat is er geconstateerd?
- ✔ Hoe schat je zelf de ernst van het incident in?
- ✔ Heb je een vermoeden hoe het is ontstaan?
- ✔ Wat heb je zelf al gedaan?

Pro-tip: Let ook op eventuele externe back-upkoppelingen.

Houd vanaf dit punt ook een logboek bij van het incident.

BELANGRIJK:
- ✔ Is er al een IRP aanwezig? Zet deze dan in werking (stap 7).
- ✔ Heb je nog geen IRP? Vervolg dan met stap 4. Maar vergeet er geen werk van te maken. (Psst, onderaan dit stappenplan helpen we je op weg. 😉)

4

STAP 4 – REGISTRATIE VAN HET INCIDENT

Stel vast welk asset (computer, laptop, server) is gecompromitteerd en bekijk of andere assets in de nabije omgeving ook gecompromitteerd zijn.

Nu volgt de verdere registratie van het incident:

- ✔ Naam van het betreffende systeem, met het besturingssysteem, IP-adres, MAC-adres.
- ✔ De account - en locatiegegevens.
- ✔ Welk netwerksegment betreft het en is deze verbonden met andere segmenten? Zo ja, hoe?
- ✔ Is de betreffende apparatuur en gebruikte software bedrijfskritisch?

Pro-tip: Als het netwerk een goed ingerichte centrale en geborgde login, zoals een SIEM, heeft dan zijn bovenstaande vragen waarschijnlijk snel beantwoord.

Maak een inschatting van hoe ernstig het incident is en wat de mogelijke impact voor de organisatie en voor klanten en andere stakeholders is. Let op: kijk eerst of het mogelijk is om een inschatting te maken. Dit moet niet – en kan ook niet altijd –, maar zal het proces zeker helpen. 😉

5

STAP 5 – REGISTRATIE VAN DE MELDING

Registreer de melding:

- ✔ De naam van de persoon die het incident gemeld heeft.
- ✔ De contactgegevens van deze persoon.
- ✔ De tijd waarop de melding binnenkwam.
- ✔ Wie zijn er op de hoogte gesteld?

6

STAP 6 – BEPAAL HET DREIGINGSNIVEAU

Kom snel bij elkaar – telefonisch of fysiek – met alle geïnformeerde leden van het responsteam en bespreek de situatie om het dreigingsniveau te bepalen.

Pro-tip: Doe dit niet online zoals via Teams of Zoom, omdat die omgevingen ook geraakt/gecompromitteerd kunnen zijn.

Na het beantwoorden van de volgende vragen zal het dreigingsniveau en de bijbehorende responsstrategie gevolgd worden:

- ✔ Is het incident nog steeds gaande?
- ✔ Hoelang speelt het al?
- ✔ Kan het incident snel onder controle worden gebracht?
- ✔ Welke gegevens of eigendommen worden bedreigd en hoe kritisch is dat?
- ✔ Raakt het incident klanten of andere stakeholders?
- ✔ Welk systeem of welke systemen zijn aangevallen, waar bevinden zij zich fysiek en in het netwerk?
- ✔ Bevindt het incident zich binnen een vertrouwd netwerk?
- ✔ Zal onze reactie de aanvaller waarschuwen, en zo ja, doet dat ertoe?
- ✔ Wat voor soort incident is dit? Is het bijvoorbeeld een virus, malware, ransomware, intrusie, misbruik, beschadiging?

Pro-tip: Als het incident klanten of andere stakeholders direct raakt, informeer deze dan zo snel mogelijk. Houd ze op de hoogte over de eventuele consequenties en vooruitgang.

7

STAP 7 – ZET HET INCIDENT RESPONSE PLAN IN WERKING

Na het bepalen van het dreigingsniveau zal het incident response plan in werking gesteld moeten worden op het juiste dreigingsniveau.

Forensisch onderzoek nodig? Houd je dan in ieder geval aan de daarvoor geldende standaarden zoals de zeven gouden w's: Wie, Wat, Waar, Wanneer, Welke wijze, Waarmee en Waarom.

ALLE STAPPEN DOORLOPEN (OF DOORGENOMEN)?

Dit is de eerste stap om je medewerkers en IT-mensen op de hoogte te brengen wat te doen na een cyberincident. Verder bouwen aan je online verdedigingsmuur?

1. Maak een stappenplan voor de medewerkers in jullie huisstijl en tone of voice. Combineer dit bijvoorbeeld met een awareness programma.
2. Onderzoek of er een allesomvattend incident response plan aanwezig is. Als dat het geval is, beoordeel of deze quicklist daarmee matcht. Is er geen incident response plan, begin dan met het opstellen hiervan. Handige links om je hiermee te helpen:

- https://www.politie.nl/binaries/content/assets/politie/algemeen/algemeen/brochure-stappenplan-cybercrime.pdf
- https://www.digitaltrustcenter.nl/informatie-advies/incident-response-plan
- https://www.sidn.nl/nieuws-en-blogs/zo-maak-je-een-cyber-incident-response-plan

SECWATCH