

Stappenplan

Incidentmeldprocedure Cyberbeveiligingswet

Stappenplan voor het melden van cyberincidenten onder de NIS2.



INLEIDING

Dit stappenplan beschrijft wat je organisatie doet zodra er een cyberincident speelt dat onder de Cyberbeveiligingswet (Cbw) valt. De wet werkt met drie vaste termijnen: 24 uur voor een eerste waarschuwing, 72 uur voor een uitgebreidere melding en 1 maand voor het eindverslag. Dit document zet die termijnen om in een concreet proces, met bij elke stap wie er aan zet is en wat er moet gebeuren.

Gebruik dit document niet pas op het moment dat het misgaat. De eerste stap gaat over wat je vooraf regelt. Lees deze procedure dus door voordat je hem nodig hebt, en wijs de rollen alvast toe.

Voor wie is dit document

Dit stappenplan is bedoeld voor elke organisatie die onder de Cyberbeveiligingswet valt, de Nederlandse uitwerking van de Europese NIS2-richtlijn. Lever je aan een organisatie die wel onder de wet valt, terwijl je er zelf niet onder valt? Dan is dit document ook nuttig als naslagwerk, al gelden de wettelijke termijnen voor je klant en niet voor jou.

Je drie termijnen in het kort

Zodra je organisatie weet dat er een significant incident speelt, lopen er drie termijnen vanaf hetzelfde beginmoment. Binnen 24 uur stuur je een eerste waarschuwing. Binnen 72 uur volgt een uitgebreidere melding. Binnen 1 maand na die melding lever je het eindverslag in. Dit document loopt elke stap voor je langs.

Vorbereiding en het ontdekken van een incident

0

Zorg dat je klaarstaat

Voordat er een incident is, moet een aantal dingen al geregeld zijn. Dat is bewust de eerste stap in dit document: op het moment dat de klok gaat lopen, is er geen tijd meer om dit alsnog te regelen. Zorg dat je organisatie geregistreerd staat bij MijnNCSC. Inloggen op dat portaal gaat via eHerkenning op niveau EH2+, gekoppeld aan je KvK-nummer, en die aanvraag kan een paar dagen duren. Wacht daar niet mee tot je het nodig hebt. Wijs vooraf vast wie welke rol vervult bij een incident. Verderop in dit document vind je een overzicht van deze rollen. Leg vast wie mag beslissen dat een incident significant is en wie de melding indient bij MijnNCSC. Spreek ook af wie de directie informeert. Houd de contactgegevens van iedereen in dit proces actueel en controleer die een aantal keer per jaar.

1

Herken het incident en leg het beginmoment vast

Een incident kan op veel manieren aan het licht komen: een melding van een medewerker, een signaal uit je monitoring of een tip van een klant of leverancier. Zodra iemand vermoedt dat er iets mis is, meldt diegene dit intern bij de security officer of het aangewezen aanspreekpunt. Leg op dat moment de datum en tijd vast waarop je organisatie kennis heeft genomen van het incident. Dit moment is belangrijker dan het lijkt: alle drie de wettelijke termijnen lopen vanaf dit tijdstip, niet vanaf het moment waarop het incident zelf ontstond. Een technisch probleem kan al dagen spelen voordat iemand het opmerkt, en pas bij die ontdekking begint de klok te lopen.

2

Bepaal of het incident significant is

Niet elk incident hoeft je te melden. De wet spreekt van een significant incident als het je dienstverlening ernstig verstoort of financiële schade voor je organisatie veroorzaakt, of als het bij andere organisaties of personen aanzienlijke schade veroorzaakt of kan veroorzaken. De exacte drempelwaarden verschillen per sector en staan in aparte regelingen. Deze beoordeling ligt bij de security officer of CISO, in overleg met de meldfunctionaris. Twijfel je of een incident significant genoeg is, ga dan uit van het zwaarste scenario. Een melding te veel kost je een half uur werk. Een melding te weinig kan een boete opleveren, of erger, een incident dat zonder toezicht verder escaleert. Blijkt het incident niet significant, dan handel je het intern af. Je kunt het incident ook vrijwillig melden bij het CSIRT, ook al ben je daartoe niet verplicht.

De meldingen: 24 uur en 72 uur

3

Verstuur binnen 24 uur je eerste waarschuwing

Is het incident significant, dan dien je zo snel mogelijk, en in elk geval binnen 24 uur na het vastgestelde beginmoment, een eerste waarschuwing in via MijnNCSC. Met die ene melding bereik je automatisch zowel het CSIRT van je sector als de toezichthouder die voor jouw organisatie bevoegd is. Deze eerste waarschuwing hoeft nog geen volledige analyse te bevatten. Vermeld of het incident vermoedelijk het gevolg is van een moedwillige actie en of er mogelijk gevolgen zijn in andere EU-landen. Voeg ook de contactgegevens toe van degene die namens je organisatie het aanspreekpunt is. Het CSIRT reageert op zijn beurt binnen 24 uur, meestal met een eerste terugkoppeling of praktisch advies.

4

Informeer je klanten als dat nodig is

Naast de melding aan CSIRT en toezichthouder kent de wet nog een aparte verplichting. Is er sprake van een ernstige dreiging die gevolgen kan hebben voor de klanten van je dienst, dan moet je die klanten daarover informeren. Deze verplichting staat los van de drie meldtermijnen en kan dus al spelen voordat je aan de 72-uursmelding toekomt. Deze stap ligt bij communicatie, in overleg met de security officer en bij voorkeur ook een jurist. Bepaal wat klanten moeten weten om zichzelf te beschermen en communiceer dat rechtstreeks aan hen, niet pas via een openbaar bericht.

5

Verstuur binnen 72 uur je melding

Binnen 72 uur na het beginmoment volgt een uitgebreidere melding, opnieuw via MijnNCSC. Hierin werk je de eerste waarschuwing bij met een inschatting van de ernst en de gevolgen van het incident. Zijn er al technische sporen bekend die op het incident wijzen, voeg die dan toe als indicatoren van compromittering.

Ook deze melding mag een eerste inschatting blijven. Je hoeft nog geen compleet beeld te hebben.

Afhandeling en eindverslag

6

Werk het incident verder af

Terwijl de meldingen lopen, blijft het incident response team bezig met het onderzoeken en oplossen van het incident zelf. Is dat binnen een maand na de 72-uursmelding afgerond, dan ga je door naar stap 7. Is het incident na die maand nog niet afgehandeld, dan lever je op dat moment een voortgangsverslag in met de stand van zaken tot dan toe. Je gaat vervolgens door met de afhandeling. Het definitieve eindverslag volgt dan binnen een maand nadat het incident is opgelost.

7

Lever binnen 1 maand het eindverslag in

Uiterlijk een maand na je melding, of bij een langere afhandeling een maand na afronding van het incident, lever je het eindverslag in. Hierin beschrijf je wat er is gebeurd en wat de vermoedelijke oorzaak was. Geef ook aan hoe ernstig het incident was en welke gevolgen het had. Sluit af met de maatregelen die je hebt genomen om het op te lossen en herhaling te voorkomen.

8

Rond het incident intern af

De wet stopt bij het eindverslag, maar een goed proces houdt hier niet op. Bespreek met het incident response team en de betrokken rollen wat er goed ging en wat beter kan. Leg vast of deze procedure moet worden aangepast en archiveer het volledige incidentdossier, zodat je er bij een volgend incident op kunt terugvallen.

Rollen en termijnen op een rij

1 Rollen in dit proces

Melder	Iedereen binnen de organisatie die een mogelijk incident opmerkt en dit intern meldt.
Security officer of CISO	Beoordeelt of een incident significant is en beslist over escalatie naar de directie.
Meldfunctionaris	Dient de wettelijke meldingen in bij MijnNCSC en bewaakt de termijnen.
Incident response team	Onderzoekt en verhelpt het incident en levert de inhoud voor elke melding.
Communicatie	Informeert klanten bij een ernstige dreiging, in overleg met de security officer en juridisch.
Directie	Eindverantwoordelijk en wordt geïnformeerd zodra een incident significant blijkt.
Juridisch (indien beschikbaar)	Toetst de klantcommunicatie en het eindverslag.

2 Je drie termijnen op een rij

TERMIJN	WAT JE DOET	WAAR NAARTOE
24 uur	Eerste waarschuwing: vermoedelijke oorzaak, grensoverschrijdende gevolgen, contactpersoon.	MijnNCSC (CSIRT en toezichthouder)
72 uur	Melding: inschatting van ernst en gevolgen, indicatoren van compromittering indien bekend.	MijnNCSC (CSIRT en toezichthouder)
1 maand	Eindverslag: volledige beschrijving, oorzaak, ernst, gevolgen en genomen maatregelen.	MijnNCSC (CSIRT en toezichthouder)

Deze procedure is gebaseerd op de Cyberbeveiligingswet en de toelichting van NCSC, RDI en NCTV. Laat het onderdeel over het informeren van klanten (stap 4) beoordelen door een jurist voordat je deze procedure in gebruik neemt, en vul de rollen in met de functies die binnen jouw organisatie bestaan.

Klaar voor de volgende stap?

Goed voorbereid is het halve werk

Als het goed is, heb je na deze stappenplan een beter beeld van wat jouw organisatie te wachten kan staan. Misschien kun je met een gerust hart verder. Misschien zijn er nog een paar aandachtspunten. Of misschien denk je vooral: hier moeten we iets mee.

Transparant

We leggen keuzes, risico's en oplossingen altijd begrijpelijk uit.

Betrouwbaar

We kiezen technologie die bewezen veilig, duurzaam en stabiel is.

Waakzaam

We signaleren risico's en denken vooruit, in plaats van af te wachten.

Vragen over de incidentmeldprocedure?



Aron

Jouw aanspreekpunt voor NIS2

Weet je niet zeker of jouw aanpak voldoet, of wil je inzicht krijgen in wat NIS2 van jouw organisatie verwacht bij een beveiligingsincident? We denken graag met je mee. Samen bekijken we jouw situatie en bespreken we welke vervolgstappen passen bij jouw organisatie.

[Plan een gesprek in](#)

BEREIKBAAR

Ma–vr, 08.00–17.30 uur

BEL ONS

085 273 58 18

STUUR EEN MAIL

hellop@inventit.nl