NIS2 Incident Response Starter Kit.

Een praktische gids voor de 24- en 72-uurs meldplicht

Cyberincidenten komen nooit gelegen. Met NIS2 komt daar een extra realiteit bij: je moet niet alleen reageren, je moet ook binnen strikte termijnen rapporteren. De vraag is dus niet alleen: kunnen we dit incident oplossen? Maar vooral: kunnen we onder druk de juiste feiten verzamelen en tijdig melden?

In de praktijk missen veel organisaties geen compleet securityprogramma, maar een paar cruciale bouwstenen. Duidelijk eigenaarschap. Een getest responseproces. Inzicht in welke informatie wanneer nodig is. Deze starter kit helpt je om incident response praktisch en uitvoerbaar in te richten. Zo bescherm je je operatie, voldoe je aan de NIS2-meldplicht en beperk je de impact.

Wat NIS2 van je verwacht

Onder NIS2 moet je kunnen aantonen dat je:

- ✓ Cyberincidenten detecteert en effectief afhandelt
- ✓ Incidenten behandelt als bedrijfsrisico, niet alleen als IT-probleem
- ✓ Binnen 24 uur na ontdekking van een significant incident een eerste melding doet
- ✓ Binnen 72 uur een vervolgmelding indient met feitelijke informatie en een eerste impactanalyse
- ✓ Technische, juridische en bestuurlijke besluitvorming coördineert

Dit vraagt om voorbereiding. Niet tijdens het incident, maar daarvoor.

Jouw 3-stappen actieplan

Stap 1

Wijs duidelijk eigenaarschap toe

De eerste uren bepalen in grote mate de uiteindelijke impact van een incident. Onduidelijkheid over verantwoordelijkheden leidt tot vertraging, en vertraging vergroot de schade. Leg daarom vooraf vast wie verantwoordelijk is voor:

- Incidentleiding en coördinatie
- Technisch onderzoek en containment
- Besluitvorming rond business en risico
- Interne en externe communicatie
- Regulatorische rapportage en documentatie

Wanneer rollen en taken helder zijn vastgelegd, kan de organisatie direct handelen in plaats van eerst verantwoordelijkheden te moeten afstemmen.

Stap 2

Maak een beknopt maar werkbaar incident response plan

Een effectief incident response plan hoeft geen uitgebreid handboek te zijn. Het doel is duidelijkheid en houvast op het moment dat de druk hoog is. Zorg dat het plan minimaal beschrijft:

- Hoe incidenten worden gedetecteerd en geëscaleerd
- Wie bepaalt of een incident als significant wordt aangemerkt
- Welke rollen en verantwoordelijkheden gelden tijdens een incident
- Hoe containment en onderzoek worden gestart
- Hoe bewijs en loggegevens worden veiliggesteld
- Verzameling info voor 24/72u-melding

Stap 3

Voer één tabletop oefening uit

Een tabletop oefening van enkele uren levert vaak meer inzicht op dan maanden beleidsontwikkeling. Door een realistisch scenario te doorlopen, wordt zichtbaar hoe het proces in de praktijk werkt. Kies bijvoorbeeld een ransomware-scenario en toets gezamenlijk:

- Wie wordt geïnformeerd en hoe snel
- Wie in de eerste uren beslissingen neemt
- Welke acties in de eerste vier uur worden uitgevoerd
- Welke informatie na 24 uur beschikbaar zou moeten zijn
- Waar eventuele hiaten bestaan richting de 72-uursmelding

Op deze manier worden zwakke plekken zichtbaar.

Als je maar 5 dingen doet

Wanneer je snel stappen wilt zetten, begin dan met deze vijf acties:

1. Benoem een Incident Lead en een plaatsvervanger.
2. Leg vast wat binnen jouw organisatie als een significant incident geldt.
3. Stel een feitenchecklist op voor de 24-uursmelding.
4. Zorg dat loggegevens en identiteits-activiteiten centraal beschikbaar zijn.
5. Test deze maand één realistisch scenario.

Veelvoorkomende hiaten in de praktijk

In de praktijk zien wij regelmatig dat:

- Er in de eerste uren geen duidelijk aangewezen incidentverantwoordelijke is
- Incident response plannen die nooit zijn getest
- Technische teams die focussen op herstel, terwijl meldingsinformatie ontbreekt
- Bewijs wordt overschreven of niet beschikbaar is wanneer toezichthouders vragen stellen
- Directieleden onvoldoende zicht hebben op welke beslissingen wanneer nodig zijn

Hoe Eye Security je ondersteunt bij NIS2 readinesss

Eye Security ondersteunt organisaties in heel Europa met praktische incident response en continue detectie. Dat doen we onder meer met:

- 24/7 detectie en response via ons Europese Security Operations Centre
- Praktische incident response planning in lijn met NIS2 verwachtingen
- Voorbereiding op 24 en 72 uur rapportage, inclusief wat je moet verzamelen, wanneer en uit welke bron
- Hands on ondersteuning bij onderzoek en containment tijdens echte incidenten
- Versterking van basismaatregelen die impact, downtime en rapportagestress beperkenind

Wil je sparren over je incident response planning of 24/7 monitoring?

Over Eye Security

Eye Security helpt kleine en middelgrote bedrijven proactief cyberrisico's identificeren en operationele weerbaarheid versterken. Het bedrijf combineert als één van Europa's voornaamste MDR-aanbieders AI-technologie, deskundige begeleiding en geïntegreerde cyberverzekeringen in één, uitgebreide oplossing. Meer dan achthonderd organisaties in Europa vertrouwen op deze verenigde aanpak om hun digitale operaties te beveiligen.

eye.security

Incident response-hotline

Heb je te maken met een cyberincident? Bel de Eye Security Incident Response-hotline op **+31 88 644 4898** (24/7 beschikbaar) of e-mail het IR-team via **cert@eye.security** voor minder urgente zaken.