Cyberfusion

Incidentendraaiboek voor bureaus

Versie: 1.0
Augustus 2026

Als bureau lopen er bij een incident twee klokken tegelijk: die van je klanten, die willen weten of hun data veilig is, en die van NIS2, met harde meldtermijnen. Een draaiboek dat je vooraf klaarlegt, scheelt in het heetst van de strijd kostbare minuten. Hieronder een basisdraaiboek dat je naar je eigen situatie aanscherpt.

T=0

Detecteer & bepaal de scope

Bevestig dat er echt iets aan de hand is en wijs één incidentcoördinator aan. Degene die het lek als eerst heeft opgemerkt is vaak de meest geschikte persoon: die weet het meest. Waar zit het: één klantsite, een gedeelde server, of je DNS- en domeinbeheer? De scope bepaalt alles wat hierna komt.

Direct

Perk in & informeer klanten

Beperk de schade: isoleer getroffen systemen, roteer sleutels en wachtwoorden, en blokkeer verdachte toegang. Laat getroffen klanten meteen weten dat er iets speelt, ook al weet je nog niet alles — het beste via een statuspagina, zodat je iedereen tegelijk up-to-date houdt zonder ze dood te spammen. Zo'n statuspagina zet je het best nu op, zodat klanten die bij voorbaat weten te vinden. Leg elke stap vast (tijdstip, actie, wie) — dat heb je straks nodig voor de meldingen. Ook is het zaak dat je actuele contactgegevens van klanten hebt, maar periodiek verifiëren is bij bureaus meestal niet nodig — tenzij jullie niet op periodieke basis contact hebben met alle klanten.

≤ 24 u

Vroege waarschuwing

Stuur binnen 24 uur een 'early warning' naar het NCSC. Nog niet alle details nodig; het gaat alleen nog om 'er speelt iets ernstigs'.

≤ 72 u

Volledige melding

Stuur binnen 72 uur de uitgebreide incidentmelding naar het NCSC. Zijn er persoonsgegevens gelekt? Dan meld je datzelfde datalek meestal ook binnen 72 uur bij de Autoriteit Persoonsgegevens (AVG).

Herstel

Herstel veilig

Zet de site terug vanaf een schone back-up, update het CMS en de plug-ins, en verifieer dat er geen achterdeur is achtergelaten (let op bekende infecties in bijvoorbeeld WordPress).

≤ 1 mnd

Eindrapport & evaluatie

Lever binnen een maand het eindrapport bij het NCSC: oorzaak, impact en genomen maatregelen. Evalueer intern wat je structureel verandert, zodat een incident van deze orde niet meer voorkomt. Dit hoeft niet ingewikkeld te zijn: ga bij elkaar zitten, neem de toedracht van het incident stap voor stap door, en bedenk bij iedere stap en actie wat beter kan.

Pas dit basisdraaiboek aan op je eigen systemen, contactpersonen en escalatiepaden voordat je het opslaat als het officiële draaiboek.

Wat ons échte managed-hosting-platform Core voor je overneemt.

Klinkt dit als veel werk? Dat hoeft het niet te zijn. Het grootste deel gaat over goede afspraken en een betrouwbare hostingpartij die het zware werk — beveiliging, monitoring, incidentrespons, DNS — overneemt. Op Core zijn deze security-basics standaard goed geregeld:

01 / 04

Dagelijkse malware-scan

Elk project wordt dagelijks gescand op malware, backdoors en verdachte bestandswijzigingen, met extra aandacht voor bekende infecties in veelgebruikte CMS-en zoals WordPress. Vinden we iets, dan hoor je het direct.

02 / 04

Security.txt voor al je projecten

Voorzie al je sites in één handeling van een security.txt-policy, zodat veiligheidsonderzoekers weten hoe ze een lek bij je kunnen melden. Handmatig op tientallen sites inloggen om een bestand te uploaden hoeft niet.

03 / 04

Scans op internetstandaarden

Laat elk domein scannen op moderne internetstandaarden zoals IPv6, DNSSEC, RPKI, DMARC en TLS. Je ziet meteen wat voldoet en wat je moet aanpakken, ook voor klanten die dat vereisen (zoals (semi-)overheid).

04 / 04

ISO 27001-gecertificeerd

Een onafhankelijke auditor controleert onze beveiliging elk jaar. Let wel: een certificaat zegt niet álles over echte beveiliging — lees meer in ons artikel over ISO-certificering.

Hoe je een lek voorkomt.

01 / 06

Beveiligingsbewustzijn

De duurste firewall helpt niet als iemand de deur openhoudt voor een vreemde. De meeste incidenten beginnen niet met een spectaculaire hack, maar met een verkeerde klik. Maak je team doorlopend bewust van phishing, social-engineering en privacy, zodat security top-of-mind blijft bij elke dagelijkse beslissing.

02 / 06

Identiteitsverificatie

Laat gevoelige verzoeken — confidentiële informatie opvragen, een wijziging laten doorvoeren — altijd via een beveiligd kanaal lopen, niet zomaar via mail of telefoon. Iedereen kan tenslotte net doen alsof die de baas is.

03 / 06

Losse servers voor losse doeleinden

Draaien DNS, mail, web en database op één server, dan geeft één kritieke kwetsbaarheid toegang tot alles: een lekke mailserver wordt zo een gelekte klantdatabase. Zet services zo veel mogelijk op aparte servers, zodat een inbraak in de ene niet overslaat naar de ander. Op Core is dat standaard makkelijk te regelen.

04 / 06

Database-encryptie 'at rest'

Versleutel je databases op de disk. Komt iemand aan de rauwe databasebestanden, dan is de data onleesbaar en dus onbruikbaar. In Core zet je dit direct aan.

05 / 06

Inzicht in je software en versies

Welke CMS'en, plug-ins en software draaien er, in welke versie, op welke server, voor welke klant? Kun je dat niet binnen een paar minuten beantwoorden, dan ben je te laat zodra er een kritiek lek opduikt. Houd een actueel overzicht van je hele inventaris bij, zodat je bij een kwetsbaarheid meteen weet wát je moet patchen en waar.

06 / 06

Meerdere bronnen, jaarlijkse review

Volg via meerdere kanalen welke kwetsbaarheden verschijnen, en evalueer jaarlijks of je nog de juiste bronnen volgt. Betrouwbare bronnen zijn onder andere security.nl en de NCSC Community.