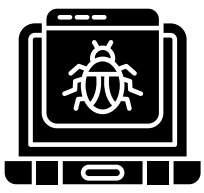
Volg deze 8 stappen bij een CYBERSECURITY INCIDENT

HERKEN OF UW SITE GEHACKT IS

Uw webshop kan gehackt zijn als u veiligheids-waarschuwingen krijgt van uw anti-virus, browser of Google. Ook bij onbekende bestanden, gebruikers of code in uw CMS of ongebruikelijke serveractiviteiten.



CONTACTEER UW IT-PARTNERS

Uw webbouwer en hostingprovider hebben de nodige expertise om een oordeel te vellen of er effectief een incident is, wat de aard van het risico is en hoe groot de omvang is.

HAAL UW WEBSHOP OFFLINE

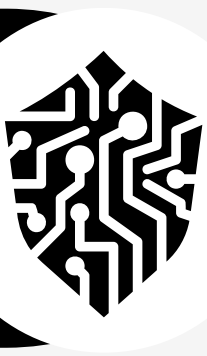
Is er effectief een cybersecurity incident vastgesteld? Om verdere schade te voorkomen, is het verstandig uw website tijdelijk offline te halen. Wijzig ook alle paswoorden van beheerders op uw website en servers.

GOEDE COMMUNICATIE

Respecteer deze volgorde van communicatie: Informeer achtereenvolgens uw leidinggevende, medewerkers, stakeholders, partners, klanten, pers. Communiceer proactief en transparant.

VERWITTIG BEVOEGDE INSTANTIES

Center for Cybersecurity Belgium - CERT.BE
Diefstal van (persoons)gegevens? Verwittig de gegevensbeschermingsautoriteit.

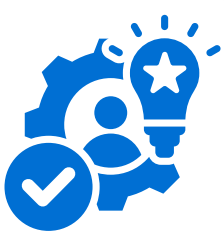


KLACHT INDIENEN BIJ DE POLITIE

Dien zo snel mogelijk een klacht in bij de politie. Zo kan er een proces verbaal opgesteld worden van de gepleegde feiten.

ANALYSE & HERSTEL

Specialisten zullen de geïnfecteerde site en server onderzoeken op sporen naar de ingang en oorsprong van de cyberaanval. Daarna zullen ze deze herstellen zodat uw systemen terug operationeel kunnen worden. Vraag nadien ook een malware-controle aan bij Google.



INCIDENTEN VOORKOMEN

Zorg dat het CMS waarmee uw webshop gebouwd is, steeds up to date blijft. Installeer automatische updates of sluit een SLA af met uw webbouwer die steeds uw webshop up-to-date moet houden.

Meer weten over dit topic?

fox & fish cyberdefense
beschermt terwijl u digitaliseert