

Gratis checklist

10-puntencheck voor uw website

Deze lijst kunt u zelf nalopen, in ongeveer een uur. U heeft er geen technische kennis voor nodig. Vink af wat klopt. Twijfelt u bij een punt, vraag het dan aan uw bouwer of hostingpartij.

Eerlijk vooraf

Deze check maakt veel zwakke plekken kleiner, maar is geen test. Wat een aanvaller op úw website kan doen, ziet u pas als iemand het echt probeert. Achteraan leest u wanneer een test zinvol is.

1

Alles is bijgewerkt

De meeste inbraken gebruiken een bekend lek waarvoor al een update bestond.

- ☐ Platform, thema en plug-ins of apps staan op de nieuwste versie.
- ☐ Beveiligingsupdates worden binnen een week geïnstalleerd, door u of uw bouwer.

2

Alleen de plug-ins die u gebruikt

Elke plug-in of app is extra code waar een fout in kan zitten.

- ☐ Plug-ins of apps die u niet meer gebruikt, zijn verwijderd (niet alleen uitgezet).
- ☐ Alles komt uit de officiële winkel of van een bekende maker.

3

Tweestapsverificatie overal

Een gestolen wachtwoord alleen is dan niet genoeg om binnen te komen.

- ☐ Aan voor het beheer van uw website of webshop.
- ☐ Aan voor uw hostingpartij, uw domeinnaam en uw zakelijke e-mail.

4

U weet wie er toegang heeft

Oude accounts van ex-medewerkers of een vorig bureau worden vaak vergeten.

- ☐ Iedereen heeft een eigen account; niemand deelt een inlog.
- ☐ Accounts die niet meer nodig zijn, zijn verwijderd.
- ☐ Medewerkers hebben alleen de rechten die ze nodig hebben.

5

Sterke, unieke wachtwoorden

Hergebruikte wachtwoorden worden als eerste geprobeerd.

- ☐ Elk account heeft een lang, uniek wachtwoord, bewaard in een wachtwoordmanager.
- ☐ Er bestaat geen account met een standaardnaam zoals "admin" en een simpel wachtwoord.

6

Back-ups die u kunt terugzetten

Een back-up waarvan u niet weet of hij werkt, is een gok.

- ☐ Er wordt automatisch elke dag een back-up gemaakt.
- ☐ Een kopie staat buiten uw eigen server, bijvoorbeeld bij een andere dienst.
- ☐ Iemand heeft het terugzetten minstens één keer echt geprobeerd.

7

Kortingscodes met grenzen

Verkoopt u online? Een code zonder grenzen kan duizenden keren gebruikt of gecombineerd worden.

- ☐ Elke code heeft een einddatum en een maximum aantal keer gebruik.
- ☐ Codes zijn niet te raden en niet onbedoeld te stapelen.

8

Betalen via uw betaalprovider

Verkoopt u online? Bestellingen die als betaald staan terwijl er niets betaald is, kosten u direct geld.

- ☐ Klanten betalen via een erkende betaalprovider; u bewaart zelf geen betaalkaartgegevens.
- ☐ Uw bouwer heeft bevestigd dat een bestelling pas op “betaald” springt als de betaalprovider dat meldt.

9

Geen technische foutmeldingen

Een foutmelding met technische details vertelt een aanvaller waar hij moet zoeken.

- ☐ Een verkeerd adres of een fout in een formulier toont een nette, gewone melding.
- ☐ De ontwikkel- of debugstand staat uit op de live website.

10

Hosting en domein op orde

Uw hostingpartij en domeinnaam zijn de fundering onder uw website.

- ☐ De hele website werkt via https, met een geldig certificaat.
- ☐ Uw hostingpakket en servertaal worden nog ondersteund en bijgewerkt.
- ☐ U weet hoe u uw hostingpartij bereikt als er iets misgaat.

Wanneer laat u het testen?

Website Security Check

Snel weten waar u staat

Een geautomatiseerde scan die wij daarna met de hand nalopen. Geen pentest: we proberen niet zelf in te breken. Rapport binnen 24 uur.

- U twijfelde bij meerdere punten hierboven.
- U wilt een nulmeting voor uw bouwer.

Pentest Website of Pentest Plus

Weten wat een aanvaller echt kan

Wij proberen met de hand in te breken, zoals een aanvaller dat zou doen. Met rapport, bewijs en een hertest.

- Uw website of webshop heeft maatwerk, klantaccounts of koppelingen.
- Een klant, partner of verzekeraar vraagt om een test.
- U heeft een incident gehad of een grote wijziging gedaan.

Altijd met toestemming

Wij testen alleen na schriftelijke toestemming van de eigenaar van het systeem. Draait uw website bij een hostingpartij of platform, dan regelen we samen ook hun akkoord.

Liever even overleggen?

Een intake van 30 minuten is gratis en vrijblijvend. Plan die via blackboxcyber.nl/contact of bel +31 485 234 002. U krijgt na het gesprek één vaste prijs op papier.

Versie 1.0 – oktober 2026. Deze checklist mag u vrij delen, ongewijzigd en met bronvermelding.