Digiweerbaar.nl

GEANONIMISEERD VOORBEELD - ALLE GEGEVENS ZIJN FICTIEF

DOMEINSCAN RAPPORTAGE

voorbeeld.example

Voorbeeldorganisatie

TYPE RAPPORT	Illustratief voorbeeld
INHOUD	Alleen de basisopzet

Technische uitvoering
Digiweerbaar.nl

Dit document bevat geen echte scanresultaten

MANAGEMENTSAMENVATTING

Wat de scan van buitenaf zag

EEN OOGOPSLAG

Deze voorbeeldscan laat zien hoe publiek zichtbare beveiligingssignalen overzichtelijk worden samengevat. De aantallen, prioriteiten en teksten op deze pagina zijn uitsluitend illustratief.

FICTIEVE BEVINDINGEN PER PRIORITEIT

1	2	3	6
Hoog	Midden	Laag	Goed

Belangrijkste conclusie

Een rapport maakt zichtbaar welke onderdelen eerst aandacht vragen en welke instellingen al goed staan.

Begin hier

1. Bespreek de hoogste prioriteit met uw ICT-partner.
2. Laat wijzigingen gecontroleerd uitvoeren en testen.
3. Plan een herhaalmeting om verbetering zichtbaar te maken.

Beperkt voorbeeld

Een volledig rapport bevat aanvullende detailpagina's, bewijs en toelichting.

GEANONIMISEERD VOORBEELD

MANAGEMENTSAMENVATTING

Hoe staat het domein ervoor?

E-mailbeveiliging

AANDACHT

Laat zien of e-mailinstellingen voldoende helpen tegen misbruik en spoofing.

Website en TLS

AANDACHT

Vat zichtbare signalen rond versleuteling, software en beveiligingsheaders samen.

DNS en domein

BASIS OP ORDE

Controleert openbare domein- en certificaatsignalen op hoofdlijnen.

Externe signalen

GEEN DIRECT SIGNAAL

Bundelt aanvullende openbare signalen zonder in systemen in te loggen.

Wat al goed is

- Versleutelde verbinding actief
- Certificaat geldig
- Geen direct openbaar leksignaal

Geen technische details in dit voorbeeld

Domeinnamen, configuraties, bewijsregels en leveranciersinformatie zijn bewust weggelaten.

GEANONIMISEERD VOORBEELD

ILLUSTRATIEVE BEVINDING

Voorbeeld van een detailpagina

AANDACHT

FICTIEF I GEEN TECHNISCH BEWIJS OPGENOMEN

E-mailauthenticatie kan strenger

Wat zien we?

Een openbare instelling lijkt minder streng dan gewenst. In een echt rapport staat hier de concrete waarneming.

Waarom is dit belangrijk?

Een aanvaller kan proberen een organisatie geloofwaardig na te bootsen. Sterkere instellingen verkleinen dat risico.

Wat kunt u doen?

Laat uw ICT-partner de huidige configuratie beoordelen, wijzigingen gecontroleerd uitvoeren en de werking daarna opnieuw testen.

TECHNISCHE ONDERBOUWING WEGGELATEN

Een klantversie bevat hier concrete signalen en vervolgadvies.

Alleen bedoeld om het concept te begrijpen

Dit voorbeeld is geen scan, audit, advies of bewijs van de veiligheid van enig domein.