Bijlage 20

Technische eisen ICT Staatsbosbeheer ten behoeve van aansluiten en benaderen webwinkel via netwerk Staatsbosbeheer

Nr.	**Webwinkel - informatiebeveiliging**
1.	Inschrijver en later Opdrachtnemer is bekend met de wetgeving bescherming persoonsgegevens en heeft procedures beschikbaar indien er een melding dient plaats te vinden.
2.	De beherende partij / hostende partij van de webwinkel beschikt over een ISO27001 of een minimaal gelijkwaardig certificaat
	Webwinkel - beschikbaarheid
3.	Met betrekking tot de beschikbaarheid van het systeem geldt het volgende: - Beschikbaarheidsvenster: 00-24.00, 365 dagen per jaar; - Beschikbaarheidseis: 97%; - Ultimo mag de Productie omgeving (inclusief onderliggende infra) in een jaar tijd maximaal 60 uur niet beschikbaar zijn tussen 09.00 en 17.00. Dit afgezien van de afgestemde onderhouds-vensters.
4.	Het datacenter waar de module gehost wordt bevindt zich binnen de Europese Economische Ruimte.
	Webwinkel – Web en portal
5.	De Opdrachtnemer monitort de webomgeving dagelijks en schakelt indien nodig extra capaciteit bij om de webdienst naar behoren te laten werken.
6.	De Opdrachtnemer stelt in productie één versie beschikbaar van de dienst aan de klanten en medewerkers van Staatsbosbeheer.
7.	De Opdrachtnemer stelt de eerstvolgende versie op tijd beschikbaar aan een klein deel van de gebruikers om een gebruikersacceptatie (GAT) mogelijk te maken.
8.	De verbinding van en naar de website dient beveiligd en versleuteld te zijn d.m.v. geldige certificaten en TLS verbinding over TCP poort 443.
9.	Medewerkers van Opdrachtgever (Staatsbosbeheer) hebben een eigen inlog op het portal en kunnen beheer uitvoeren over gebruikersaccounts en aangeboden diensten in het systeem. Er is binnen het portal een verschil in machtiging mogelijk.
10.	Het inlogaccount is niet herleidbaar naar Staatsbosbeheer. Eventueel biedt Opdrachtnemer een mogelijkheid tot SSO. Bij het gebruik van SSO hanteert Opdrachtgever aanvullende eisen.

11.	De oplossing kan worden benaderd via elke moderne standaard-browser (marktconform) en kan daarmee zonder plug-ins juist, volledig en optimaal worden gebruikt, onafhankelijk van de onderliggende hardware (waarbij de term "modern" niet blijft hangen op het moment van de initiële ingebruikname maar voortdurend de actualiteit volgt).
	Webwinkel – Webserver
12.	Opdrachtgever streeft naar een langdurige score van 100% op internet.nl, ook in de verdere toekomst. De immer verdergaande beveiligingseisen zullen doorgaand met de Opdrachtnemer besproken worden.
13.	De website is bereikbaar via IPv4 en IPv6.
14.	HTTP compressie dient uitgeschakeld te zijn op de webservers.
15.	Alle websites en portalpagina's dienen ten alle tijden te bereiken zijn via HTTPS poort 443 en geen andere poort.
16.	Indien niet alle informatie via een beveiligde verbinding wordt uitgewisseld, vindt er een permanente redirect plaats van http naar https.
17.	De webserver waarop de webapplicatie draait dient voorzien te zijn van een HSTS-policy. Dit zorgt er voor dat bij een terugkerend bezoek van een klant de browser direct naar HTTPS verbind.
18.	De webapplicatie ondersteunt TLS 1.2 en TLS 1.3. Deze versies van SSL/TLS bieden betere veiligheidsvoorzieningen.
19.	De webserver(s) ondersteunen alleen voldoende veilige cipher suites. Voor meer informatie zie 'TLS-richtlijnen van NCSC', richtlijn B2-1 t/m B2-4. https://www.ncsc.nl/documenten/publicaties/2021/januari/19/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2.1
20.	De webserver(s) ondersteunen voldoende veilige Diffie-Hellman-parameters voor sleuteluitwisseling. Voor meer informatie zie 'TLS-richtlijnen van NCSC', richtlijnen B4-1 t/m 4-2. https://www.ncsc.nl/documenten/publicaties/2021/januari/19/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2.1
21.	Er mag geen gebruik gemaakt worden van SSLv1, SSLv2, SSLv3, TLS1.0 en TLS1.1.
22.	TLS compressie dient uitgeschakeld te zijn.
23.	De webserver waarop de webapplicatie draait dient voorzien te zijn van een HSTS-policy. Dit zorgt ervoor dat bij een terugkerend bezoek van een klant de browser direct naar HTTPS verbindt.
24.	De portal en webdienst dienen minimaal aan A+ te scoren op de Qualys SSL labs – SSL Server Test website.
25.	Het is niet toegestaan om additionele applicaties te leveren voor bijvoorbeeld beheer in de on-premise omgeving van Staatsbosbeheer. De Opdrachtnemer garandeert dat alle functionaliteiten

	volledig zijn ondergebracht in de website / portal / beheerwebsite. Er dient een webapplicatie geleverd te worden waar onder verstaan wordt dat deze via een webbrowser ontsloten kan worden.
26.	Opdrachtnemer verplicht zich tot het gebruiken van veilige cookies of apps.
27.	De webapplicatie maakt gebruik van invoervalidatie om verdachte tekens, karakters of commando's uit te sluiten.
28.	De Opdrachtnemer kan en gaat gebruik maken van een gedelegeerd sub-domein {subdomein}.staatsbosbeheer.nl en voert daar ook het technisch beheer over uit. Staatsbosbeheer blijft eigenaar van {subdomein}.staatsbosbeheer.nl.
29.	De webserver biedt veilig ingestelde X-Frame-Options aan
30.	De webserver biedt X-Content-Type-Options aan.
31.	De webserver biedt veilig ingestelde X-XSS-Protection aan.
32.	De webserver biedt Content-Security-Policy (CSP) aan.
33.	De webserver biedt Referrer-Policy aan
	Webwinkel – DNS
34.	Opdrachtnemer gaat er mee akkoord dat het DNS beheer en hosting niet wordt overgedragen aan de Opdrachtgever. Opdrachtgever blijft eigenaar van het domeinnaam.
35.	DNS aanvragen en wijzigingen verlopen via Staatsbosbeheer ICT.
36.	Staatsbosbeheer gebruikt DNSSec op het domein @staatsbosbeheer.nl en alle andere domeinnamen die gehost gaan worden bij Opdrachtnemer. Opdrachtnemer ondersteunt DNSSec en alle aanpalende instellingen en configuraties die daarmee gemoeid zijn. Denk daarbij aan DANE, DMARC en DKIM.
37.	Op domeinnamen van Opdrachtnemer die gebruikt worden door Staatsbosbeheer medewerkers dient ook DNSSec ingesteld en ondersteund te worden. Denk daarbij aan domeinnamen waar functioneel beheerders toegang tot het CMS krijgen.
	Webwinkel – Certificaten
38.	Staatsbosbeheer is eigenaar van certificaten en vraagt alle benodigde certificaten aan. De Opdrachtnemer levert tijdig de CSR's aan met als basis de volgende instellingen: Organisatie Unit (OU): BackOffice ICT Organisatie (O): Staatsbosbeheer Locatie (L): Amersfoort Provincie (S): Utrecht Land (C): NL
39.	Voor afgeschermde ontwikkel en testomgevingen zijn Let's Encrypt of gelijksoortige certificaten

	toegestaan die de Opdrachtnemer zelf mag aanvragen. Voor Productie systemen die publiekelijk toegankelijk zijn dienen altijd minimaal bedrijfsgevalideerde certificaten aangevraagd te worden bij Staatsbosbeheer.
40.	Certificaten die nodig zijn voor de werking van functionaliteiten op @staatsbosbeheer.nl worden op verzoek door Staatsbosbeheer aangeschaft en overhandigd. Het is niet toegestaan om zelf certificaten aan te vragen en/of gebruik te maken van Let's Encrypt of gelijksoortige diensten. De aanschafkosten voor deze certificaten worden door Staatsbosbeheer gedragen.
	Webwinkel – Web en API
41.	Bij gebruik van API is het geboden webproduct via REST webservices te benaderen en gebruikt daarbij JSON als in- en uitvoer formaat.
42.	De REST webservice is voldoende gedocumenteerd zodat interfacebouwers in staat zijn om gebruikt te maken van de REST API.
43.	De verbinding van en naar de REST API dient beveiligd en versleuteld te zijn d.m.v. geldige certificaten en TLS verbinding.
	Webwinkel – Mail
44.	Om systeemmeldingen uit de webapplicatie te kunnen versturen dient de Opdrachtnemer gebruik te maken van een eigen subdomein wat in gedelegeerd beheer is bij Opdrachtgever, ({subdomein}.staatsbosbeheer.nl). Opdrachtnemer kan bijvoorbeeld mails versturen vanuit info@{subdomein}.staatsbosbeheer.nl. Denk daarbij aan: aanmelden nieuw account, wachtwoord wijzigen, bevestiging bestelling, etc.
45.	Opdrachtnemer dient TLSA-record op te nemen in DNS ten aanzien van DANE zodat de authenticiteit van een certificaat ook via het DNS TLSA-record gevalideerd kan worden.
46.	Indien er bulk e-mail verstuurd wordt vanuit de webapplicatie dient deze verspreid te worden over uren heen om spamfilters niet op ratelimits te triggeren.
47.	Opdrachtnemer dient echtheidswaarmerken op te nemen tegen e-mailvervalsing. (DMARC, DKIM en SPF). Dit zorgt ervoor dat ontvangers daardoor betrouwbaar phishing- of spammails, die onze domeinnaam ({subdomein}.staatsbosbeheer.nl) in hun afzenderadres misbruiken, kunnen scheiden van echte e-mails.
	Webwinkel – Back-up and disaster recovery
48.	Het is mogelijk dat het datacenter waar Opdrachtnemer de omgeving van Opdrachtgever host problemen ondervindt, zoals algehele regionale stroomuitval, aardbeving, overstroming etc., maar ook uitval van core componenten, zoals core routers of primaire verbindingen naar het internet. Dit noemen wij een calamiteit. Bij calamiteiten geldt de volgende beschikbaarheidseis: RTO: Maximale duur van onbeschikbaarheid omgeving 1 werkdag RPO: Maximaal dataverlies 1 dag
49.	De Opdrachtnemer zorgt dat op verzoek van Staatsbosbeheer een backup kan worden

	teruggeplaatst, iedere nacht tot maximaal 7 dagen terug.
50.	De Opdrachtnemer garandeert dat Bron-data & back-updata zich nooit op dezelfde fysieke datacenter locatie bevinden.
	Webwinkel – Security infrastructuur
51.	De Opdrachtnemer garandeert dat de firewall bescherming biedt tegen virussen, malware, trojans en exploits op bekend en onbekend internet verkeer.
52.	De Opdrachtnemer rapporteert 1 x per 3 maanden een overzicht met daarin de volgende gegevens: Aantal gedetecteerde aanvallen; Type aanvallen; Succesfactor van de aanval; Genomen maatregelen om de aanvallen af te slaan; Aantal onsuccesvolle aanmeldingen;
53.	De Opdrachtnemer is in staat om rapportages te overleggen over uptime, performance, login info, back-up en beveiligingsincidenten. De Opdrachtnemer is in staat om verschillende rapportages te maken indien Staatsbosbeheer daar om vraagt.
54.	De Opdrachtnemer overlegt minimaal 1 keer per jaar een rapport waaruit blijkt dat de Opdrachtnemer en haar producten en diensten voldoen aan de laatste beveiliging niveaus voor websites, infrastructuur en certificaten.
55.	Staatsbosbeheer voert periodiek pentesten uit. De Opdrachtnemer is akkoord met deze pentesten en tekent daartoe op verzoek een verklaring van geen bezwaar.