Adviesrapport – Informatiebeveiligings- en privacycertificeringen voor Boomtag

Inleiding

Boomtag gebruikt2 NFC tags die worden geïntegreerd in sportgerief. Via deze technologie kunnen gebruikers productinformatie en eigen administratie van het product raadplegen. Ook is het een manier om diefstal te preventeren. De verwerking en opslag van deze data gebeurt via Amazon Web Services (AWS).

Door juist deze data die verwerkt wordt, waaronder mogelijk ook persoonsgegevens, is het voor Boomtag belangrijk om te voldoen aan bekende internationale normen voor informatiebeveiliging en privacy. Niet enkel dit belangrijk voor hun eigen cyberweerbaarheid en databeheer, maar ook voor samenwerkingen met andere bedrijven. Het in bezit zijn van gekende certificeringen is nuttig om vertrouwen te creeren bij partners.

We weten dat Booomtag ernaar streeft om de ISO 27001 norm te behalen, maar willen ook hun bekend maken met de verschillende certificeringen waar zij daarnaast nog naar kunnen streven. Dit adviesrapport geeft een overzicht van relevante certificeringen en aankomende Europese wetgeving op het gebied van cybersecurity.

Aanbevolen en toepasselijke internationale certificeringen

Certificering	Omschrijving	Relevantie voor Boomtag
ISO/IEC 27001	Internationaal erkende standaard voor informatiebeveiliging. Richt zich op het implementeren van een Information Security Management System (ISMS).	Garandeert een gestructureerde aanpak voor beveiliging van NFC- en clouddata.
ISO/IEC 27701	Uitbreiding op ISO 27001 gericht op privacybeheer en AVG-naleving.	Toont aan dat Boomtag persoonsgegevens zorgvuldig verwerkt volgens Europese privacywetgeving.
SOC 2 (Type II)	Beoordeelt interne beveiligingsmaatregelen m.b.t. cloudsystemen.	Relevant omdat Boomtag gebruikmaakt van AWS en hiermee aan kan tonen dat dataverwerking betrouwbaar en veilig verloopt.
ISO/IEC 27017 & 27018	Richtlijnen voor respectievelijk cloudbeveiliging en bescherming van persoonsgegevens in de cloud.	Direct toepasbaar op Boomtag's cloudomgeving binnen AWS.
ISO/IEC 22301	Richt zich op bedrijfscontinuïteit en crisismanagement.	Versterkt de weerbaarheid van Boomtag tegen storingen of cyberincidenten.

Minder gekende, toepasselijke certificeringen voor Boomtag's technologie

Certificering	Toepassing
ISO/IEC 30141 (IoT Reference Architecture)	Richtlijn voor veilige IoT-architecturen. Helpt bij het ontwerpen van betrouwbare en schaalbare NFC-systemen met ingebouwde beveiliging ("security by design").
CE-markering (met Radio Equipment Directive – RED)	Wettelijk vereist voor draadloze NFC-apparatuur. Bewijst dat de producten voldoen aan veiligheids- en privacyvereisten van de EU.

Opkomende Europese norm: EU Cyber Resilience Act (CRA)

De EU Cyber Resilience Act (CRA) is een nieuwe Europese wetgeving die het beveiligen van digitale producten verplicht maakt. De wet zal naar verwachting tussen 2025 en 2027 volledig van kracht worden.

Belangrijkste verplichtingen voor Boomtag:

- Beveiliging moet ingebouwd zijn vanaf het ontwerpstadium (security by design).
- Fabrikanten moeten een actief vulnerability managementproces bijhouden.
- Software-updates en patchmanagement zijn verplicht gedurende de levensduur van het product.
- Producten krijgen een CE-markering op basis van cybersecurityeisen.

Relevantie: Boomtag's NFC-apparaten en bijbehorende software vallen onder de categorie "producten met digitale elementen". Door nu al te werken volgens ISO 27001, 27701 en 30141, voldoet Boomtag grotendeels aan de principes die de Cyber Resilience Act vereist. Door nu al te streven naar het voldoen van de CRA-vereisten voorkomt Booomtag risico's zoals vertraging en duurdere (compliance) kosten. Ook zal Booomtag een concurrentievoordeel hebben tegen bijvoorbeeld bedrijven buiten de EU, die nog weinig kennis van de CRA hebben.

Als Booomtag wel al streeft naar de bestaande certificeringen die hierboven zijn gelijst, zal het niet moeilijk zijn om te voldoen aan de Europse norm omdat er grotendeels is op voortgebouwd

Conclusie en advies

Boomtag bevindt zich op het snijvlak van hardware, software en cloudtechnologie. Om vertrouwen te wekken bij klanten, partners en toezichthouders is het sterk aan te raden om te investeren in een geïntegreerd beveiligings- en privacykader.

Doel	Aanbevolen certificering / norm	Opmerking
Basisinformatiebeveiliging	ISO/IEC 27001	Fundamentele standaard; basis voor alle andere.
Privacy en AVG-naleving	ISO/IEC 27701	Zorgt voor vertrouwen en naleving van Europese wetgeving.
Cloudbeveiliging (AWS)	ISO/IEC 27017 & 27018 + SOC 2	Sluit direct aan bij AWS-compliance en dataverwerking.
IoT/NFC-beveiliging	ISO/IEC 30141 + CE/RED	Technische beveiliging van apparaten en communicatie.
Toekomstige EU-wetgeving	EU Cyber Resilience Act (CRA)	Wordt verplicht; richt je processen hier nu al op in.

Met deze certificeringen positioneert Boomtag zich als een veilig, toekomstgericht en privacybewust technologiebedrijf binnen de Europese markt.