10 geheimen van veilige software op maat

Cruciale stappen voor het ontwikkelen en onderhouden van beveiligde software

1. Security by Design vanaf dag een

Beveiliging is geen laag die je achteraf toevoegt. Het moet in de architectuur, de datamodellen en de codebase zelf zijn ingebakken vanaf de eerste schets.

2. Maatwerk versus Off-the-shelf

Standaardsoftware is een geliefd doelwit voor geautomatiseerde exploits omdat een enkel lek miljoenen installaties treft. Goed ontworpen maatwerksoftware biedt een veel kleiner aanvalsoppervlak.

3. Veilige integraties en API-beveiliging

Elke koppeling tussen softwarepakketten is een potentieel risico als authenticatie, rate limiting en data-validatie niet strikt zijn ingericht.

4. De tien kernprincipes voor een veilige softwarestack

1. Inleiding: de evolutie van cyberdreigingen in moderne webapplicaties.
2. Evolutie van IT-security: van perimeterverdediging naar zero trust.
3. Maatwerk vs standaardpakketten: risico-analyse en aanvalsoppervlak.
4. Security by design: threat modeling en veilige coderingsrichtlijnen.
5. De 6 meest voorkomende fouten bij softwarebeveiliging en hoe ze te voorkomen.
6. Cloudsecurity: encryptie in transit en at rest, veilige geheimen en IAM.
7. Infrastructuur en netwerksegmentatie: minimaliseer laterale beweging.
8. Gegevensbescherming en GDPR/NIS2-compliance in de praktijk.
9. Onafhankelijke security audits en penetratietesten.
10. Beveiliging na oplevering: monitoring, patching en incident response.

Contacteer DMVH voor een vrijblijvende security review van uw softwarestack.