

Beveiliging integreren in de designfase: hoe begint u eraan?

03 september 2025, 08:24

Tatiana Galibus

Volg ons stappenplan om de ingebouwde veerkracht van moderne software te vergroten

De volgende feiten zijn algemeen bekend: 1. Cyberbedreigingen worden alsmaar frequenter en complexer. Er zit dus niets anders op dan onze inspanningen op het gebied van cyberbeveiliging op te drijven. 2. Het is eenvoudiger, krachtiger en goedkoper om functionaliteiten van bij het begin in uw software te integreren dan om ze toe te voegen wanneer de software volledig ontwikkeld is.

Als u die twee zaken in overweging neemt, begrijpt u meteen het belang van ‘Security by Design’. Dat concept kan u helpen om risico's in een vroeg stadium te beperken, om uw kosten te verlagen en om het vertrouwen van gebruikers te verhogen. Voeg daarbij nog de Cyber Resilience Act en andere wetten die bedrijven dwingen om beveiliging als een integraal deel van hun ontwikkelingsinspanningen te beschouwen, en u begrijpt dat ‘Security by Design’ niet gewoon een optie is voor softwareontwikkelaars, maar een must.

Maar hoe evolueert u van uw huidige manier van werken naar een ontwerp- en ontwikkelingsomgeving die beveiliging begrijpt en integreert in de hele ontwikkelingscyclus? Het

onderstaande stappenplan kan daarbij een handig hulpmiddel zijn.

Wat is Security by Design?

Security by Design is het principe dat beveiliging vanaf de vroegste stadia in de systeemontwikkeling moet worden geïntegreerd, in plaats van het er achteraf aan te breien. Dat houdt in dat men vanaf de eerste ontwerpbeslissingen en gedurende de hele softwareontwikkelingscyclus (SDLC) rekening moet houden met potentiële dreigingen en risicobeperkende strategieën.

Het helpt u om digitale omgevingen te bouwen die veerkrachtig, conform en betrouwbaar zijn, of u nu een rudimentair SaaS-product bouwt of een grootschalige infrastructuur beheert.

Maak kennis met Acme

Om de typische workflow van Security by Design inzichtelijker te maken, nemen we u mee in het traject van een denkbeeldig softwarebedrijfje, Acme, dat werkt aan een web-app waarmee gedistribueerde teams to-dolijsten kunnen opstellen om aan samen te werken. De naam van de app is AcmeTasks. Acme wil er zeker van zijn dat hun softwareproduct veilig en schaalbaar is en beantwoordt aan nieuwe EU-regelgeving zoals NIS2 en de CRA.

Zicht op de context

Voordat Acme aan zijn ontwikkelingstraject begint, moet het inzicht verwerven in hun bedrijfsrealiteit en doelstellingen. Ze formuleren daarom een duidelijk antwoord op de volgende vragen:

- **Wat?** Ze willen een drielagige web-app bouwen (front-end, back-end, database) om to-dolijsten te beheren.
- **Voor wie?** De eindgebruikers van de web-app zijn onder meer telewerkers, kleine teams en freelancers.
- **Met welke gegevens?** E-mailadressen, gebruikerstaken, bijlagen, optionele facturatiegegevens.
- **Wat zijn de beperkingen?** De web-app moet tegen 2027 voldoen aan de CRA-normen en moet worden gemaakt door een klein team van zes ontwikkelaars.

Beveiligings- en bedrijfsdoelstellingen definiëren

Acme moet begrijpen dat hun activiteiten en beveiliging volledig op elkaar moeten worden afgestemd. Met andere woorden: beveiliging moet de bedrijfsdoelen ondersteunen, niet belemmeren.

De bedrijfsdoelstellingen: Acme heeft bepaald dat er binnen zes maanden een MVP of ‘minimum viable product’ moet worden gelanceerd. Dat product moet GDPR- en CRA-conform zijn om toegelaten te worden op de Europese markt. Daarnaast moet het voldoende veerkrachtig zijn om het vertrouwen van klanten te winnen en zo B2B-klanten aan te trekken.

Dat vertaalt zich in de volgende **beveiligingsdoelstellingen**: Acme moet de gebruikers-gegevens beschermen tegen lekken of wijziging en moet ongeoorloofde toegang tot de takenlijsten voorkomen. Bovendien moet de onderneming ervoor zorgen dat de service steeds beschikbaar blijft, zelfs bij een zware werklast en ongewoon veel webverkeer.

Dreigingsmodellen opstellen (met STRIDE)

Als u uw digitale bezittingen goed wil beschermen, moet u begrijpen aan welke gevaren ze worden blootgesteld. Daartoe kunt u gebruik maken van dreigingsmodellen, waarmee u kunt nagaan hoe een aanvaller uw systeem zou kunnen aanvallen. In het Engels heet dit ‘threat modeling’. Acme heeft besloten om STRIDE te gebruiken, een van de meest toegankelijke methoden, die zich richt op zes aanvalstypen.

De STRIDE-analyse van hun AcmeTasks-app leidt tot de identificatie van de volgende dreigingen:

- **S – Spoofing:** een aanvaller krijgt toegang door zich voor te doen als een gebruiker via een onveilige login
- **T – Tampering:** een gebruiker bewerkt de taken van een andere gebruiker met kwade bedoelingen
- **R – Repudiation:** een gebruiker wist taken en ontkent dat hij ze heeft gewist
- **I – Openbaarmaking van informatie:** taakgegevens worden onversleuteld verzonden in gewone HTTP en zijn daardoor leesbaar voor derden
- **D – Denial of Service:** de API van de app wordt overbelast met spam om taken aan te maken
- **E – Elevation of Privilege:** een gewone gebruiker verwerft admin-toegang

Beveiligingsvereisten definiëren

Op basis van het bovenstaande dreigingsmodel kunnen de Acme-ontwikkelaars beveiligingsvereisten opstellen, zoals:

- Gebruik HTTPS voor elke gegevenstransmissie
- Gebruik OAuth 2.0 voor authenticatie
- Pas rolgebaseerde toegangscontrole (RBAC) toe
- Implementeer invoervalidatie en uitvoercodering
- Log gevoelige acties voor traceerbaarheid
- Beperk het aantal toegestane verzoeksnelheden (rate limiting) om DoS tegen te gaan
- Versleutel gebruikersgegevens in rust met AES-256

Als aan die eisen wordt voldaan, worden de verschillende dreigingen sterk beperkt en zal het resulterende product gevoelig veiliger zijn.

Integreren in de SDLC

Veilig ontwikkelen en ontwerpen is een goed begin, maar daar stopt het niet. Veiligheid is geen eenmalige actie, het is een voortdurend traject. Acme's veilige ontwikkeling en ontwerp moeten deel uitmaken van een volledige softwareontwikkelingscyclus of Software Development Life Cycle (SDLC). Zo'n cyclus bestaat uit de volgende stappen:

- **Design:** waar de dreigingsmodellen en het design van de beveiligingspatronen (bv. RBAC) worden uitgewerkt
- **Ontwikkeling:** het gebruik van veilige versleutelingsnormen, zoals die in de OWASP Top 10
- **Testwerk:** inclusief statische en dynamische analyses, het scannen van afhankelijkheden enz
- **Implementatie:** bij de uitrol van het product moet er speciale aandacht worden besteed aan onder meer geheimenbeheer en CI/CD hardening
- **Onderhoud:** last but not least omvat de hele levenscyclus het jarenlange onderhoud van een draaiend systeem, geïdentificeerde kwetsbaarheden en inbreuken moeten snel en kordaat worden aangepakt met patchbeheer en incidentrespons, zo kunnen ze in de toekomst tot een nog veiliger product leiden

Uw team opleiden

Een veilige digitale omgeving vereist altijd een diepgaand beveiligingsbewustzijn. Medewerkers, eindgebruikers en ontwikkelaars/ontwerpers moeten inzicht hebben in de verschillende dreigingen en weten hoe ze ermee moeten omgaan. En omdat het bedreigings- en beveiligingslandschap voortdurend verandert, zal continu leren altijd deel uitmaken van een goede beveiligingscultuur.

Acme begrijpt dat en heeft een aantal initiatieven genomen om hun teams verder op te leiden:

- Ze geven startopleidingen over veilig ontwikkelen
- Ze organiseren workshops over dreigingsmodellen en codebeoordelingsoefeningen
- De leden van het ontwerp- en ontwikkelingsteam abonneren zich op beveiligingsbulletins (bv. CVE-feeds) om op de hoogte te blijven van de laatste nieuwigheden en trends

Nog een tip: gebruik platformen zoals CyberActive als u streeft naar EU-conforme cyberbeveiligings-opleidingen die zijn gericht op de CRA, NIS2 en best practices voor veilig programmeren.

Opvolgen, bijwerken, verbeteren

Acme weet dat de onderhoudsfase meer omvat dan alleen het opvolgen van gerapporteerde beveiligingsproblemen. Als ze willen dat hun applicatie betrouwbaar blijft, moeten ze die voortdurend en actief opvolgen om snel te kunnen reageren en alles af te toetsen. Hun proactieve beveiligingsbeleid omvat:

- Logboekregistratie en -bewaking instellen (bv. ELK-stack, Sentry)
- Logboeken controleren op verdachte activiteiten
- Regelmatig scannen op kwetsbaarheden
- Bedreigingsmodellen elk kwartaal beoordelen en herzien
- Deadlines van CRA en certificeringsstappen voorblijven

Klaar om in de voetsporen van Acme te treden? Neem contact met ons op

Security by Design draait om veerkracht, vertrouwen en levensvatbaarheid op lange termijn. Voor een bedrijf als Acme betekent vroeg investeren in gestructureerde praktijken dat ze veilig kunnen schalen, vertrouwen kunnen winnen en kunnen voldoen aan het veranderende juridische

landschap.

Hetzelfde geldt voor uw organisatie. Of het nu gaat om een eenmalige ontwikkelings-inspanning of om continu onderhoud van een ICT-infrastructuur, beveiliging moet de nodige aandacht krijgen. Ze moet ingebakken zijn in uw dagelijkse bedrijfsvoering, van de ontwerpcultuur tot de bugtracker.

En wij kunnen u helpen om dat te bereiken.

Met ons Lunch & Learn-traject leren we u hoe u uw bedrijf meer compliant maakt en beter beschermt tegen alle mogelijke bedreigingen.

Neem daarvoor contact op met het SecDes-project (‘Security by Design’) voor SaaS-ontwikkelaars en -providers.

Ook kunnen we u meer informatie geven over de hierboven beschreven stappen of over de richtlijnen en tools voor CRA-compliance en Security by Design. Neem contact op met tatiana.galibus@sirris.be en zij bezorgt u graag de gewenste informatie.

Normen en kaders voor Security by Design

Security by Design is een belangrijke vereiste geworden bij de ontwikkeling van software en digitale omgevingen. Ontwikkelaars en ontwerpers zijn verplicht aan bepaalde normen te voldoen. Gelukkig beschikken ze over tal van handige kaders en tools om hen te helpen bij hun beveiligingsinspanningen. Hieronder volgen enkele van de belangrijkste normen en kaders die de ‘Security by Design’-benadering ondersteunen:

- **CRA of Cyberweerbaarheidswet (EU, 2024):** de nieuwste wetgeving die cyberbeveiliging voor digitale producten gedurende hun hele levenscyclus verplicht
- **NIST SP 800-160:** Systems Security Engineering, richtlijnen om beveiliging te integreren in ontwikkelingsprocessen
- **OWASP SSDLC:** praktijken op het gebied van veilige softwareontwikkelingscycli
- **ISO/IEC 27034:** beveiligingskader voor toepassingen
- **Microsoft SDL:** beveiligingsontwikkelingscyclus die intern door Microsoft wordt gebruikt
- **ENISA-richtlijnen:** aanbevelingen voor cyberbeveiliging op EU-niveau

Bouw veiligheid in vanaf de eerste regel code

Wilt u veilige applicaties ontwikkelen die voldoen aan de nieuwste regelgeving zoals NIS2 en de Cyber Resilience Act? In deze masterclass krijgt u concrete handvatten en praktische

ervaring met security by design en dreigingsmodellering. Zet vandaag de stap naar robuuste, toekomstbestendige software.

Schrijf u in voor de masterclass

Auteurs



Tatiana Galibus