Whitepaper

De kracht van Threat Modeling: een veiligere digitale oplossing

iquality

Inhoudsopgave

01

Threat Modeling: verklein je digitale kwetsbaarheid

Digitale kwetsbaarheden signaleren in een vroeg stadium

In de voortdurend veranderende wereld waarin we leven is het van groot belang dat onze persoonlijke gegevens, bedrijfsgeheimen, financiële transacties en andere informatie op een veilige manier verwerkt worden. Digitale veiligheid is een belangrijk speerpunt in het ontwerpen en realiseren van digitale oplossingen.

Hoe zorgen we voor digitale veiligheid? Dat doen we door bewust te worden van de mogelijke bedreigingen waarmee we geconfronteerd kunnen worden. Threat modeling is een krachtige methode die ons helpt om vooruit te denken, onze verdediging te versterken en potentiële beveiligingsincidenten te voorkomen.

“Threat Modeling is een krachtige methode die ons helpt om vooruit te denken, onze verdediging te versterken en potentiële beveiligingsincidenten te voorkomen.”

Door deze whitepaper te lezen, leer je hoe wij threat modeling gebruiken om veilige digitale oplossingen te ontwerpen en bouwen. Daarbij zoeken we de "open eindjes" actief op om te zorgen dat er niets vergeten wordt.

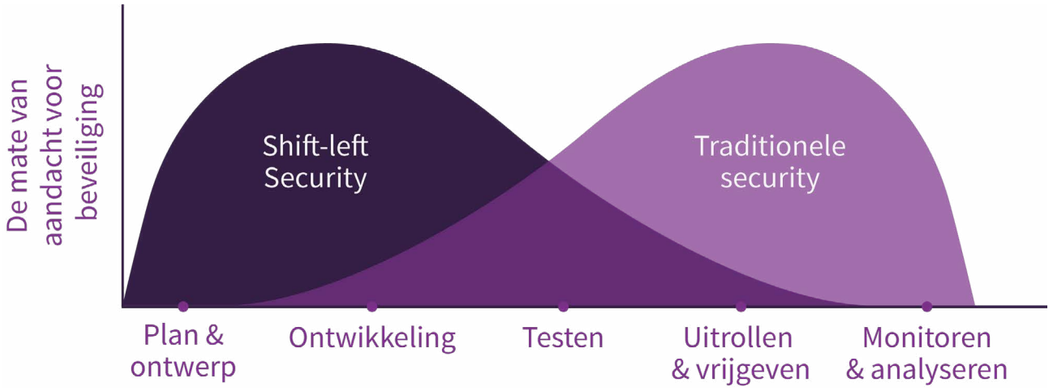
Het resultaat? Een robuuster en beter beveiligd systeem, met effectieve beveiligingsmaatregelen en geminimaliseerde risico's.

01

Shift-left security

Proactieve softwarebeveiliging

Voordat we threat modeling introduceren, laten we je eerst kennismaken met shift-left security. Shift-left security vertegenwoordigt een proactieve mindset. Het idee is om beveiligingsmaatregelen en controles al in te bouwen tijdens de ontwerpfase en gedurende het ontwikkelingsproces, in plaats van achteraf beveiligingsproblemen op te lossen. De naam 'shift-left security' zegt het daarmee al, beveiliging wordt letterlijk naar links in de ontwikkelcyclus verschoven.



Stel je voor...

Stel je een situatie voor waarin een organisatie bezig is met de ontwikkeling van een nieuwe applicatie. De organisatie heeft ervoor gekozen om pas aan het einde van het ontwikkelingsproces, net voor de implementatie, een beveiligingsbeoordeling uit te voeren.

Tijdens de beoordeling zijn er verschillende kwetsbaarheden ontdekt. Vervolgens wordt het ontwikkelteam geconfronteerd met een race tegen de klok om de beveiligingslekken op te lossen, wat helaas leidt tot vertraging in de release van de applicatie. Bovendien hebben ze te maken met een grotere complexiteit omdat de code al grotendeels is geschreven en er grote wijzigingen moeten worden doorgevoerd om de beveiligingsrisico's op te lossen (=verhoogde kosten).

Dit scenario had voorkomen kunnen worden wanneer threat modeling vanaf het plan en ontwerp werd geïntegreerd. Het ontwikkelteam had de tijd gehad om de juiste maatregelen te treffen voor zwakke punten in het systeem.

Threat Modeling als intrinsiek onderdeel van softwareontwikkeling

Door threat modeling binnen de shift-left security gedachte toe te passen, bevordert het de cultuur van 'security by design', het wordt een intrinsiek onderdeel van het ontwikkelproces. Dit zorgt ervoor dat beveiliging niet als een 'afterthought' wordt beschouwd, maar als een essentieel aspect dat vanaf de eerste stappen wordt meegenomen. Dit resulteert in een hogere kwaliteit van de software, omdat potentiële beveiligingsproblemen worden geïdentificeerd en aangepakt voordat ze kunnen escaleren.

02

Threat Modeling in vier stappen

Het Threat Modeling stappenplan

Het proces van threat modeling omvat verschillende stappen, waaronder het definiëren van de data flow van de digitale oplossing, het identificeren van mogelijke bedreigingen en kwetsbaarheden, het definiëren van maatregelen om de kwetsbaarheden te verminderen om ze vervolgens te valideren. Het is een **iteratief proces** wat zich blijft herhalen. De software wordt daarmee voortdurend beoordeeld en geëvalueerd zodat nieuwe bedreigingen en kwetsbaarheden tijdig worden herkent.

Omschrijf de data flow.
Creëer een diagram van de digitale oplossing.

Identificeer bedreigingen.
Identificeer en classificeer potentiële bedreigingen.

Beoordeel bedreigingen.
Stel vast hoe bedreigingen voorkomen kunnen worden.

Valideer maatregelen.
Valideer dat maatregelen effectief zijn geweest in het voorkomen van bedreigingen.

02 Stap 1: Omschrijf de data flow

De digitale oplossing in kaart brengen

Een belangrijk onderdeel van threat modeling is het omschrijven van de dataflow van de digitale oplossing. De gegevensstromen in het systeem worden geanalyseerd om te bepalen welke gegevens er worden verzonden, waar ze vandaan komen en waar ze naartoe gaan. De belangrijkste assets worden hiermee in kaart gebracht.

Het maken van een diagram

De data flow van de digitale oplossing wordt geschetst in een diagram, de hele digitale oplossing wordt hiermee in kaart gebracht. Onderdelen die complexer zijn worden uitgelicht en hiervoor wordt op een dieper niveau eenzelfde type diagram gemaakt.

De bouwstenen van het diagram

Onderstaande bouwstenen worden gebruikt om op een schematische wijze inzicht te geven in de opbouw van een digitale oplossing.

Een proces is een component (al dan niet maatwerk) dat taken faciliteert.

Een externe entiteit valt buiten onze eigen invloedssfeer (bijvoorbeeld een gebruiker of een externe dienst).

Data kan opgeslagen worden in bijvoorbeeld een database, zoekindex, bestand op een harddisk of cloudopslag.

Als er communicatie plaatsvindt, dan geven we dat aan met een lijn.

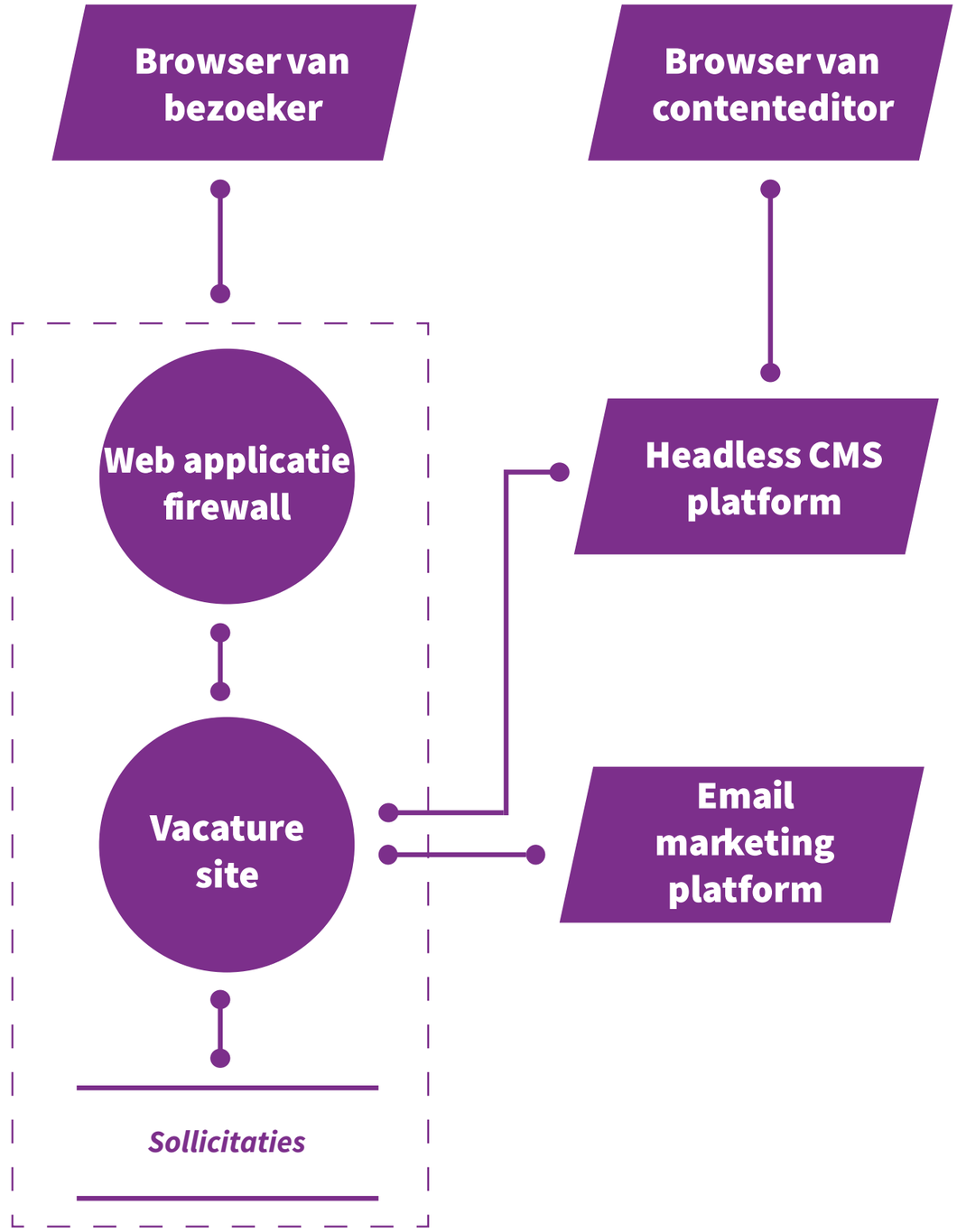
Een vertrouwensgrens geeft aan waar een scheiding tussen onderdelen die we wel en niet vertrouwen zit (bijvoorbeeld tussen een eigen netwerk en het internet).

Voorbeeld: vacaturesite

Hiernaast zie je, vereenvoudigd, hoe de verschillende bouwstenen gecombineerd worden tot een volledig dataflow diagram voor een vacaturesite. De eerste stap, en daarmee de basis voor threat modeling, is gezet!

Context voor deze digitale oplossing:

- **Vacatures worden beheerd in een extern content beheersysteem.**
- **Bezoekers kunnen vacatures inzien en solliciteren op de website.**
- **Sollicitaties worden opgeslagen en er wordt een e-mail verzonden naar een HR medewerker om deze erop te wijzen.**



02

Stap 2: Identificeer bedreigingen

Verplaatsen in een hackers' mindset

In de volgende stap wordt er gekeken naar het diagram en worden mogelijke bedreigingen bedacht. We verplaatsen ons in de mindset van een hacker en kijken hoe we de **beschikbaarheid**, **integriteit** en **vertrouwelijkheid** van het systeem kunnen schaden.

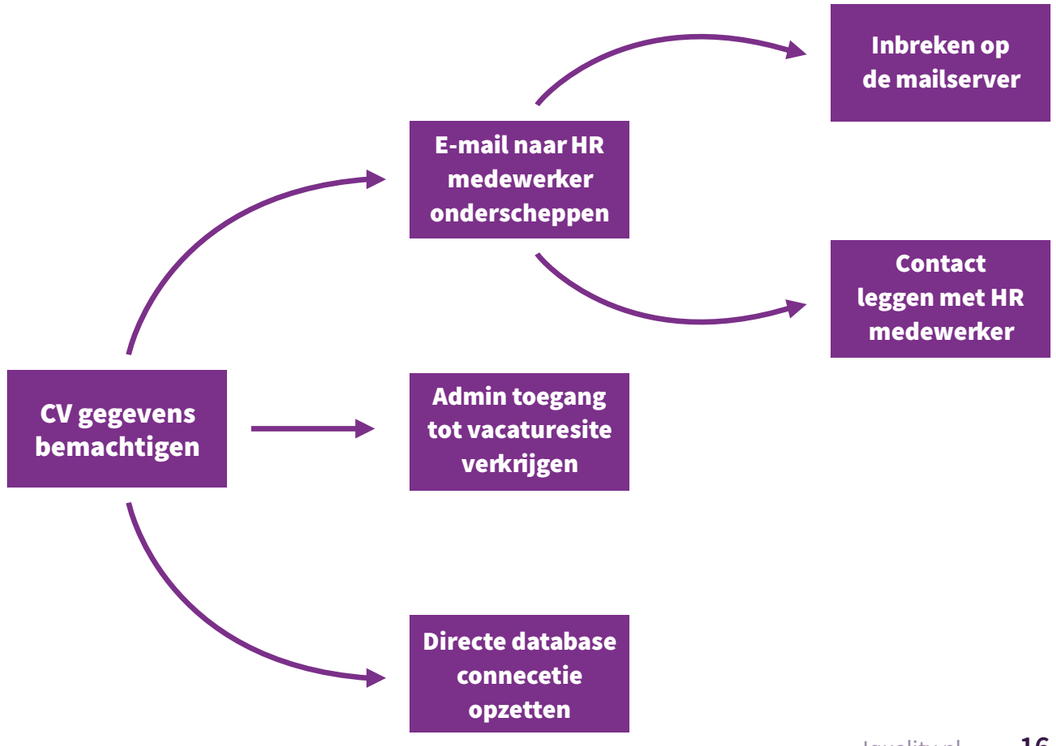
Maar er wordt ook gekeken naar wat er zou kunnen gebeuren als een incompetente of zelfs kwaadwillende eigen medewerker aan de slag zou gaan. En wat zou er kunnen gebeuren als een externe dienst waar gebruik van wordt gemaakt gehackt zou worden?

Attack tree

Een van de manieren om bedreigingen te identificeren is door gebruik te maken van zogeheten '**attack trees**'. Het is een visuele representatie van de verschillende stappen die een hacker kan zetten om een specifiek doel te bereiken. Een attack tree start daarom met het doel, ook wel het doelwit, zoals het stelen van gevoelige informatie of het verkrijgen van toegang tot een systeem. Vervolgens identificeren we de manieren waarmee een hacker het doelwit kan bereiken, bijvoorbeeld door gebruik te maken van kwetsbaarheden in software.

Voor elke mogelijkheid worden we steeds concreter en worden ze opgesplitst in sub-stappen. Deze sub-stappen worden vervolgens verder opgedeeld tot er geen verdere stappen meer mogelijk zijn.

Deze boomstructuur brengt mogelijke beveiligingsrisico's in kaart op basis van de vacaturesite op de vorige slide.



02

Stap 3: Beoordeel bedreigingen

Bedreigingen classificeren middels het STRIDE model

Na het identificeren van de bedreigingen, is het belangrijk om ze te beoordelen en de ernst ervan te evalueren. Er wordt bepaald wat de waarschijnlijkheid is dat een bedreiging zich voor gaat doen en de potentiële impact ervan op het systeem.

Dat wordt gedaan door het opstellen van een lijst waar bedreigingen worden geclassificeerd op basis van het STRIDE model.

STRIDE bestaat uit zes bedreigingscategorieën en staat daarmee voor: Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege. Elke categorie beschrijft een manier waarop een bedreiging impact heeft. "Spoofing" betekent bijvoorbeeld dat iemand zich voordoet als een ander en "Tampering" betekent dat informatie is veranderd op een schadelijke wijze.

Voorbeeld: vacaturesite risico's

De lijst wordt benaderd zoals dat vaak gebeurd in risk management processen (zie afbeelding). Voor ieder item op de lijst bepalen we:

- **Welke STRIDE categorieën van toepassing zijn.**
- **Een beschrijving van het risico.**
- **Een score die de grootte van de impact aangeeft.**
- **Een score die aangeeft hoe groot de kans is dat we getroffen worden.**
- **Een score die afgeleid is uit het voorgaande en aangeeft wat de prioriteit is.**
- **Hoe we het risico kunnen verminderen of volledig kunnen voorkomen.**

ID	S	T	R	I	D	E	Beschrijving	Impact	Kans	Prio	Maatregelen
1	X			X			CV data uit database lek	Hoog (3)	Middel (2)	6 (3x2)	Beperk toegang database met sterkere authenticatie
2					X		Site plat door DDOS aanval	Laag (1)	Middel (2)	2 (1x2)	Firewall (WAF) met DDOS beveiliging instellen
...							...	...	...	...	...

02

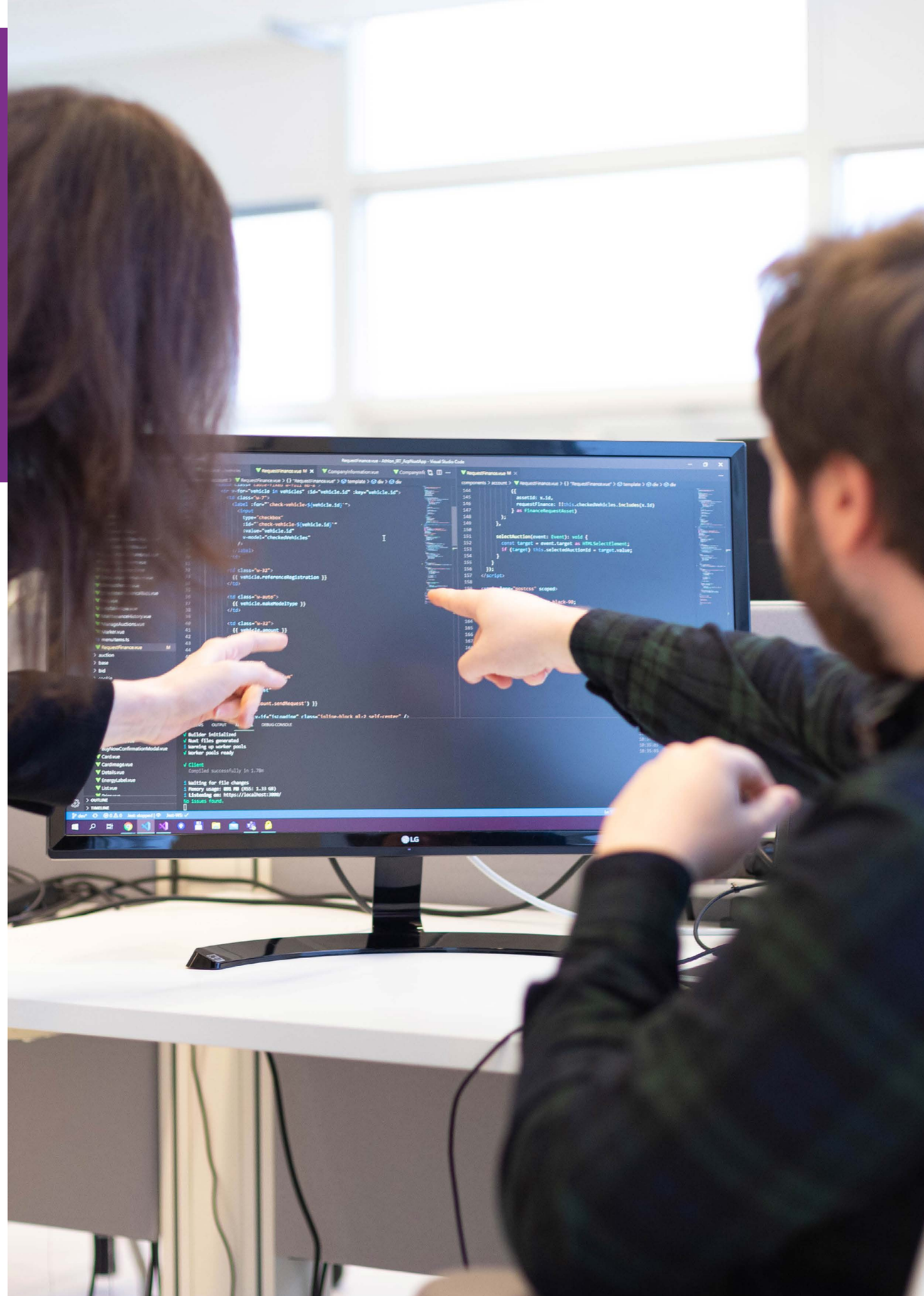
Stap 4: Valideer maatregelen

Effectieve activiteiten starten om bedreigingen te mitigeren

Ten slotte is het van belang om de genomen maatregelen te valideren. De opgestelde lijst uit stap 3 wordt gebruikt om activiteiten te starten om geïdentificeerde bedreigingen te mitigeren. Dit kan gebeuren door middel van code reviews, penetratietesten, vulnerability assessments en andere technieken om te testen of de maatregelen daadwerkelijk werken zoals verwacht.

Wanneer een van deze activiteiten is voltooid, kan het originele risico in de lijst worden bijgewerkt. Het is belangrijk dat er gecontroleerd wordt of de gemaakte wijzigingen effect hebben en of het risico hiermee voldoende is afgedekt. Er wordt opnieuw een inschatting gemaakt van de impact en de prioriteit. Indien de kans en/of impact voldoende verlaagd zijn, kan het risico geheel van de lijst gehaald worden.

Het doel van het validatie proces is om er zeker van te zijn dat de beveiligingsmaatregelen effectief zijn en om eventuele tekortkomingen te identificeren, zodat deze kunnen worden aangepakt voordat software wordt vrijgegeven.



03

De waarde van het toepassen van Threat Modeling

Welke resultaten merk jij nou écht?

1. Een veiligere digitale oplossing
Jij biedt een veiligere digitale oplossing aan aan jouw gebruikers. Het draagt bij aan een sterke reputatie als betrouwbare en veilige organisatie.

2. Het verkrijgen van certificeringen en licenties
Threat modeling past in veel gevallen goed bij de maatregelen die getroffen moeten worden voor het verkrijgen van certificeringen en licenties. Het kan bijvoorbeeld goed invulling geven aan enkele eisen voor ISO27001.

3. Verbeterde samenwerkingen binnen teams
De gezamenlijke inspanning om beveiliging te borgen zorgt voor een gedeeld begrip van informatiebeveiliging, communicatie tussen verschillende disciplines wordt daarmee gestimuleerd.

4. Het voorkomen van hoge herstel kosten
Het vroegtijdig identificeren en oplossen van beveiligingsrisico's voorkomt herstelkosten later in het ontwikkelproces.

03 Naar een betere beveiliging van jouw informatie

Threat Modeling: een waardevol onderdeel van het ontwikkelproces

Start ook met het verbeteren van de beveiliging van jouw digitale oplossing met threat modeling! Door het systematisch identificeren en analyseren van potentiële bedreigingen en kwetsbaarheden, kunnen organisaties gericht maatregelen nemen om deze te mitigeren of te voorkomen.

Wanneer threat modeling juist wordt toegepast en wordt geïntegreerd in softwareontwikkelings- en beveiligingsprocessen draagt het bij aan:

1. Veiligere digitale oplossingen;
2. Verkrijgen van certificeringen en licenties;
3. Verbeterde samenwerking;
4. Voorkomen van hoge herstelkosten.

Wil je nog meer geïnspireerd worden of persoonlijk advies ontvangen bij jouw volgende digitale uitdaging?

Neem contact met ons op!

Kudos
Robin Hermanussen
(Software Architect)
Merel IJpelaar
(Online Marketeer)

Kom met ons in contact via *INFO@IQUALITY.NL*
of bel naar +31 (0)85 080 2300

iquality

Volg ons @iquality