

## A • WAT & WAAROM

## Casus & scope

*Waar hebben we het precies over? Wat hoort er nog nét wel bij — en wat laten we bewust buiten beschouwing?*

← LESBL0K 2

## B • WIE

## Stakeholders & belangen

*Wie heeft belang, wie beslist, wie draagt het risico? Waar botsen die belangen?*

← LESBL0K 5

## C • WAT BESCHERMEN WE

## Assets & kroonjuwelen

*Wat moet beschermd worden? Nummer ze A1, A2 ... – deze nummers gebruik je de rest van de minor.*

LESBLOK 6

## Waarde & belofte

Waarom doet dit ertoe? Wat verwachten mensen stilzwijgend als ze dit gebruiken?

← LESBLOK 1

## Gebruikers & gedrag

*Wat doen mensen echt op een drukke dag? Waar snijden ze de bocht af omdat veilig te omslachtig is?*

← LESBLOK 4

## Abuse cases

Minstens drie, altijd zo: **Als** *⟨wie⟩* *⟨wat doet⟩*, **dan** *⟨welke schade⟩* **op** *⟨assetnummer⟩*.

LESBLOK 6

## BIV-profiel

Wat is hier de ergste schade: meekijken (V), gegevens die niet kloppen (I), of dat het niet werkt (B)? Zet op volgorde, mét reden.

← LESBL0K 1

## Wie zou dit misbruiken?

*Denk breed: buitenstaanders, eigen mensen, leveranciers, toeval. Wat is het motief?*

← LESBLOK 8

## Ontwerpprincipes & keuzes

Welke twee principes gelden hier? Schrijf per principe één concrete keuze: principe → dus wij kiezen ...

- LESBL0K 3

## Aannames & open vragen

*Wat hebben we aangenomen omdat het niet in de casus stond? Wat zouden we willen weten, en aan wie vragen we dat?*



## Meenemen naar week 2

Welk risico vinden we nú het scherpst, en waarom? Eén zin.



# Security Context Canvas

Referentie-uitwerking. Bewust vollediger dan wat teams in 50 minuten halen — gebruik de kwaliteitslat, niet dit vel, als norm.

CASUS

Wijkzorg-app “Naaste”

TEAM

voorbeeld

VERSIE

1.0

DATUM

—

A · WAT & WAAROM

B · WIE

C · WAT BESCHERMEN WE

Casus & scope1

De app, de koppeling met de apotheek, de telefoons van verzorgenden en de externe bouwer/beheerder.

**Buiten scope:** het personeelssysteem — dat raakt de cliëntzorg niet rechtstreeks.

← LESBLOK 2

Stakeholders & belangen4

Cliënt · mantelzorger · verzorgende · teamleider · externe bouwer · apotheek · zorgverzekeraar · FG.

**Botsing:** teamleider wil snel inloggen op de gang; de FG wil sterke authenticatie.

← LESBLOK 5

Assets & kroonjuwelen7

**A1** zorgnotities · **A2** medicatiegegevens ★ · **A3** identiteit/toegang mantelzorger ★

**A4** telefoons verzorgenden · **A5** chatgeschiedenis · **A6** vertrouwen van cliënten ★

★ = kroonjuweel

← LESBLOK 6

Waarde & belofte2

Mantelzorgers voelen zich betrokken en gerustgesteld.

Stilzwijgende belofte: **“wat hier staat klopt, en alleen wij kunnen het zien.”**

Beide helften van die belofte kunnen los sneuvelen — dat is het gesprek.

← LESBLOK 1

Gebruikers & gedrag5

Verzorgende met acht cliënten op een ochtend blijft ingelogd; telefoon ligt in de auto.

Notities worden 's avonds thuis uit het hoofd bijgewerkt — dat raakt **integriteit**, niet vertrouwelijkheid.

← LESBLOK 4

Abuse cases8

– **Als** iemand zich als familielid voordoet en toegang krijgt, **dan** leest een buitenstaander mee **op A3, A1**

– **Als** een telefoon met actieve sessie wordt gestolen, **dan** liggen notities van meerdere cliënten op straat **op A4, A1, A5**

– **Als** de apotheekkoppeling stil verouderde medicatie doorgeeft, **dan** handelt een verzorgende op onjuiste info **op A2**

← LESBLOK 6

BIV-profiel3

**I → V → B.**

Onjuiste medicatienotities geven direct schade aan een cliënt; dat weegt zwaarder dan een lek.

Voor de cliënt zélf ligt V mogelijk hoger — dat spanningsveld benoemen.

← LESBLOK 1

Wie zou dit misbruiken?6

– nieuwsgierige buurman die zich voordoet als familie

– ex-partner die via mantelzorger-toegang wil meelesen

– medewerker van de bouwer met productietoegang

– verzorgende die per ongeluk bij de verkeerde cliënt schrijft

← LESBLOK 8

Ontwerpprincipes & keuzes9

**Least privilege** → een mantelzorger ziet alleen zijn eigen naaste, en alleen de zorgmomenten.

**Secure by default** → automatisch uitloggen na inactiviteit.

Ruil: kost gemak voor de verzorgende. Bewust genomen.

← LESBLOK 3

Aannames & open vragen

We nemen aan dat de bouwer géén toegang heeft tot productiedata — dat weten we niet. **Vraag aan de teamleider:** wie kan er bij de gegevens van de externe partij?

Meenemen naar week 2

Scherpste risico: **A3** — mantelzorger-toegang toekennen is nu een menselijke beslissing zonder controle, en dat opent alle andere assets.