

STRIDE-light Canvas

Zes vragen aan hetzelfde systeem. Werk met het Security Context Canvas van week 1 ernaast: de assetnummers (A1, A2 ...) van toen zijn hier de verwijzing. Niet elk vak hoeft vol — een leeg vak mét reden is ook een antwoord.

Het systeem in blokjes

Teken maximaal zes blokjes: mensen, plekken waar gegevens staan, en partijen buiten je eigen organisatie. Verbind ze met pijlen — elke pijl is iets wat verstuurd, opgehaald of gedeeld wordt.

← BLOK 3

Vertrouwensgrenzen & assets

Zet een streep waar gegevens van de ene partij naar de andere gaan. Welke assetnummers steken die grens over?

← WEEK 1 · CANVAS

S

Zich voordoen als

SPOOFING

Kan iemand zich voordoen als een ander — als gebruiker, als collega, of als een systeem waarop wij vertrouwen?

WIE · WAT · ASSET

★ TOP-3

T

Ongemerkt wijzigen

TAMPERING

Kan er onderweg of achteraf iets veranderen aan de gegevens? Merkt iemand het als ze niet meer kloppen?

WIE · WAT · ASSET

★ TOP-3

R

Achteraf ontkennen

REPUDIATION

Kunnen we later nog aantonen wie wat deed? Of kan iemand met droge ogen zeggen: dat was ik niet?

WIE · WAT · ASSET

★ TOP-3

I

Meekijken

INFORMATION DISCLOSURE

Wie kan iets zien wat niet voor hem bedoeld is — ook per ongeluk, en ook binnen de eigen organisatie of bij een leverancier?

WIE · WAT · ASSET

★ TOP-3

D

Eruit liggen

DENIAL OF SERVICE

Wat gebeurt er als dit een dag niet werkt of vastloopt? Wat doen mensen dán — en welk risico ontstaat daardoor?

WIE · WAT · ASSET

★ TOP-3

E

Meer rechten krijgen

ELEVATION OF PRIVILEGE

Kan iemand meer dan bedoeld — door een rol die stilletjes meegroeit, een uitzondering die blijft staan, of een vergeten account?

WIE · WAT · ASSET

★ TOP-3

Van dreiging naar ontwerpkeuze — top 3

Drie dreigingen die je nu aanpakt. De maatregel is een keuze, het requirement is de afspraak die je erover vastlegt.

DREIGING (LETTER + ASSET)	MAATREGEL	REQ.	HOE MERKEN WE HET?

Leeg gelaten, aangenomen, meegenomen

Welk vak bleef leeg, en waarom is dat een keuze en geen vergeetpost? Wat namen we aan, en aan wie vragen we dat na?

STRIDE-light Canvas

Referentie-uitwerking op dezelfde doorlopende casus als het week 1-canvas. Bewust vollediger dan wat teams in 50 minuten halen — twee regels per vak is een prima opbrengst.

CASUS	TEAM	VERSIE	DATUM
Wijkzorg-app “Naaste”	voorbeeld	1.0	—

Het systeem in blokjes

Mantelzorger
eigen telefoon

→

App “Naaste”
telefoon verzorgende

→

Zorgdossier
backend + database

↔

Apotheek
medicatie-feed, 's nachts

↔

Externe bouwer
beheer & support

← BLOK 3

Vertrouwensgrenzen & assets

– telefoon ↔ backend — A1 A2 A5

– zorgorganisatie ↔ apotheek — A2

– zorgorganisatie ↔ externe bouwer — A1 A2

– verzorgende ↔ mantelzorger (rolgrens) — A3

← WEEK 1 · CANVAS

S

Zich voordoen als

SPOOFING

★ Uitnodigingslink voor een mantelzorger gaat via WhatsApp en is aan niemand gebonden — wie hem eerst opent, is “de familie” A3 A1

– De apotheek-feed komt binnen op één gedeeld token: wie het token heeft, ís de apotheek A2

– Verzorgende leent haar telefoon “even snel” uit aan een collega; het systeem ziet één persoon A4 A1

T

Ongemerkt wijzigen

TAMPERING

★ De nachtelijke medicatiebatch loopt half vast; de app toont de dosering van gisteren zonder enige waarschuwing A2

– Notities worden 's avonds thuis uit het hoofd bijgewerkt — geen kwade wil, wel onjuiste inhoud A1

– Een notitie kan zonder spoor worden overschreven; wat er eerst stond is weg A1

R

Achteraf ontkennen

REPUDIATION

– Eén teamtelefoon, vier verzorgenden: achteraf niet te zien wie de notitie schreef A1 A4

– De bouwer beheert met een gedeeld admin-account; “iemand van support” is geen naam A1 A2

– Mantelzorger-toegang wordt telefonisch geregeld; wie hem toekende staat nergens vast A3

I

Meekijken

INFORMATION DISCLOSURE

★ Gestolen telefoon met een actieve sessie: de notities van acht cliënten liggen op straat A4 A1 A5

– Support van de bouwer kan in productie zoeken op naam, zonder dat iemand dat terugziet A1

– Pushmeldingen tonen de cliëntnaam op een vergrendeld scherm, in de bus zichtbaar voor de buurman A1

D

Eruit liggen

DENIAL OF SERVICE

– Apotheekkoppeling ligt eruit → de verzorgende werkt verder op geheugen en papier; niet de app is het risico, maar wat mensen dán doen A2

– Golf aan resetverzoeken loopt via de teamleider; die zet de controle tijdelijk uit om door te kunnen A3

– Er is met de bouwer niets afgesproken over hersteltijd; “zo snel mogelijk” staat in geen contract A2 A6

E

Meer rechten krijgen

ELEVATION OF PRIVILEGE

– Mantelzorger krijgt er “zorgmomenten” bij en ziet daarmee ongemerkt het hele dossier A3 A1

– Verzorgende kan zichzelf toevoegen aan cliënten buiten de eigen route — handig bij invallen, nooit teruggedraaid A1

– Het account van een vertrokken verzorgende staat nog open; niemand is eigenaar van het afsluiten A1 A3

Van dreiging naar ontwerpkeuze — top 3

DREIGING (LETTER + ASSET)	MAATREGEL	REQ.	HOE MERKEN WE HET?
S · uitnodiging niet persoonsgebonden A3	koppeling alleen na bevestiging door de teamleider, op één geverifieerde persoon	REQ-01	maandlijst nieuwe koppelingen naar de teamleider
T · stille batchfout medicatie A2	app toont “laatst bijgewerkt”; ouder dan 24 uur = blokkeren, niet tonen	REQ-02	alarm op een uitgebleven of halve feed
I · telefoondiefstal met actieve sessie A4 A1	automatisch vergrendelen, sessie aan het toestel binden, wissen op afstand	REQ-03	melding bij een sessie op een onbekend toestel

★

Leeg gelaten, aangenomen, meegenomen

Aanname: de bouwer ziet geen productiedata — onbevestigd. Vraag aan de teamleider: welke logging staat er op supporttoegang?

Bewust klein gehouden: D — een dag geen app is hier hinderlijk, geen ramp; het echte risico zit in wat mensen dan doen (staat bij D).

Mee naar blok 5: REQ-01 t/m 03 in de traceability-matrix, met de assetnummers uit week 1.

🚩

WK1 CONTEXT → WK2 RISICO → WK3 GOVERNANCE → WK4 ONTWERP → DOSSIER VOORBEELD

Minor Secure by Design · Avans Hogeschool · securebydesign.nu