

Attack-tree Challenge

Eén doel van de aanvaller bovenaan, drie routes eronder. Elk pad krijgt één zin “hoe dan?” en een assetnummer uit het week 1-canvas — een pad zonder assetnummer is een mening. Punten voor wat plausibel is, extra punten voor wat niemand anders bedacht.

CASUS

TEAM

DOELKAART

DATUM

Het doel van de aanvaller

Schrijf het doel van je doelkaart hier over, in de ik-vorm van de aanvaller. Eén zin, geen middel — “ik wil ...”, niet “ik hack ...”.

RAAKT DE ASSETS

1

Wie wil dit, en waarom?

Persona non grata: wie is het, wat levert het hem op, en wat heeft hij ervoor over? Geen hoodie — een naam, een motief en een grens.

2

← BLOK 1 · AANVALLERSDENKEN

DE BOOM · DRIE ROUTES NAAR HETZELFDE DOEL per blad: hoe dan (één zin) · welk assetnummer · EN of OF ten opzichte van het blad erboven

Via de mens

Vragen, vertrouwen, meekijken, meelopen. Geen enkele regel code.

M1

HOE DAN? · ASSET

EN / OF ✓ ○ ★ ○

Via het apparaat & de techniek

Toestellen, sessies, accounts, netwerk — en alles wat blijft openstaan.

T1

HOE DAN? · ASSET

EN / OF ✓ ○ ★ ○

Via de keten, het proces & de organisatie

Leveranciers, beheer, afspraken die er niet zijn, rechten die blijven staan.

K1

HOE DAN? · ASSET

EN / OF ✓ ○ ★ ○

M2

HOE DAN? · ASSET

EN / OF ✓ ○ ★ ○

T2

HOE DAN? · ASSET

EN / OF ✓ ○ ★ ○

K2

HOE DAN? · ASSET

EN / OF ✓ ○ ★ ○

M3

HOE DAN? · ASSET

EN / OF ✓ ○ ★ ○

T3

HOE DAN? · ASSET

EN / OF ✓ ○ ★ ○

K3

HOE DAN? · ASSET

EN / OF ✓ ○ ★ ○

M4

HOE DAN? · ASSET

EN / OF ✓ ○ ★ ○

T4

HOE DAN? · ASSET

EN / OF ✓ ○ ★ ○

K4

HOE DAN? · ASSET

EN / OF ✓ ○ ★ ○

Het snijpunt — één maatregel, meerdere takken

Welke maatregel haalt in één klap de meeste bladeren weg? Noteer welke, en hoe je zou merken dat iemand het tóch probeert.

MAATREGEL	SNIJDT AF	HOE MERKEN WE HET?

→ BLOK 9 · RISICOPROFIEL

Te mooi om waar te zijn

Welk pad sneuvelde bij “hoe dan?” — en wat maakte het onrealistisch: te duur, te veel geluk, of te veel mensen die moeten meewerken?

Jurypunten

✓ plausibel pad — 1 punt

★ plausibel én uniek — 1 punt extra

✕ snijpunt mét detectie — 3 punten

TOTAAL

Attack-tree Challenge

Referentie-uitwerking op de doorlopende casus van week 1. Bewust vollediger dan wat een team in de challenge haalt — twee sterke bladeren per route is een prima opbrengst. Let op de bladeren die aan elkaar vastzitten (EN): daar zit het snijpunt.

CASUS

Wijkzorg-app “Naaste”

TEAM

voorbeeld

DOELKAART

D1

DATUM

—

Het doel van de aanvaller

“Ik wil lezen hoe het met haar gaat — wanneer de zorg langskomt, wat er in de notities staat — **zonder dat iemand doorheeft dat ik meekijk.**”

Niet: “ik wil de app hacken”. Het doel is informatie over één persoon, niet het systeem.

RAAKT DE ASSETS **A1 ZORGNOTITIES** · **A3 MANTELZORGERTOEGANG** · **A4 TELEFOONS** · **A5 CHAT**

1

Wie wil dit, en waarom?

Ex-partner van een cliënt. Motief: controle houden — weten wie er komt en wanneer zij alleen is.

Middelen: veel tijd, kent de familie, mag zichzelf voorstellen als bezorgde naaste. Grens: hij wil niet betraptd worden en niets doen dat strafbaar oogt.

2

← BLOK 1 · AANVALLERSDENKEN

DE **BOOM** · DRIE ROUTES NAAR HETZELFDE DOEL ✓ = plausibel volgens de jury · ★ = geen ander team had dit · EN = alleen samen met het blad erboven

Via de mens

Vragen, vertrouwen, meekijken, meelopen. Geen enkele regel code.

Belt de teamleider als “bezorgde zoon” en vraagt mantelzorgertoegang. Koppelen gaat telefonisch; er is geen controle op wie hij is. **M1**

A3 A1 **0F** ✓ ● ★ ○

Vraagt in de familie-app of iemand “de link” doorstuurt. De uitnodiging is aan niemand gebonden: wie hem opent, is de familie. **M2**

A3 **0F** ✓ ● ★ ●

Wacht bij de bushalte op de verzorgende: pushmeldingen tonen de cliëntnaam op een vergrendeld scherm. **M3**

A1 **0F** ✓ ● ★ ○

Praat een verzorgende aan op de sportclub: “hoe gaat het met haar?” Zij vertelt het uit betrokkenheid. **M4**

A1 A6 **0F** ✓ ● ★ ○

Via het apparaat & de techniek

Toestellen, sessies, accounts, netwerk — en alles wat blijft openstaan.

Neemt de telefoon van de verzorgende mee uit de onafgesloten auto tijdens het huisbezoek. **T1**

A4 **0F** ✓ ● ★ ○

De sessie stond nog open — geen automatische vergrendeling. Acht dossiers, inclusief chat, staan meteen open. **T2**

A1 A5 **EN OP T1** ✓ ● ★ ○

De teamtelefoon heeft één pincode die iedereen kent en die op de achterkant staat geplakt. **T3**

A4 A1 **0F** ✓ ● ★ ○

De oefenomgeving voor nieuwe medewerkers draait op een kopie van echte dossiers en staat open op internet. **T4**

A1 **0F** ✓ ● ★ ○

Via de keten, het proces & de organisatie

Leveranciers, beheer, afspraken die er niet zijn, rechten die blijven staan.

Meldt zich bij de externe bouwer als medewerker met een probleem; support zoekt in productie mee op cliëntnaam. **K1**

A1 **0F** ✓ ● ★ ○

Support werkt op één gedeeld admin-account: achteraf is “iemand van support” de enige naam die je vindt. **K2**

A1 A2 **EN OP K1** ✓ ● ★ ○

Zijn nieuwe partner werkte er tot vorige maand. Haar account staat nog open; niemand is eigenaar van het afsluiten. **K3**

A1 A3 **0F** ✓ ● ★ ●

De apotheekkoppeling loopt op één gedeeld token; wie het token heeft, ziet de medicatie per cliënt. **K4**

A2 **0F** ✓ ● ★ ○

Het snijpunt — één maatregel, meerdere takken

MAATREGEL	SNIJDT AF	HOE MERKEN WE HET?
Sessie aan het toestel binden, automatisch vergrendelen, meldingen zonder naam	T1+T2, T3, M3	melding bij een sessie op een onbekend toestel
Mantelzorger koppelen alleen na bevestiging door de teamleider, op één geverifieerde persoon	M1, M2	maandlijst nieuwe koppelingen naar de teamleider
Support op eigen naam, productie alleen na akkoord, offboarding met eigenaar	K1+K2, K3	wekelijkse export van supportzoekopdrachten op cliëntnaam

→ BLOK 9 · RISICOPROFIEL

Te mooi om waar te zijn

Inbraak bij de bouwer, 's nachts, in het serverhok. Sneuvelde bij “hoe dan?”: deze aanvaller wil niet betraptd worden — en één telefoontje (M1) werkt beter.

Zero-day in de app kopen. Plausibel voor een andere aanvaller, niet voor deze: geld noch toegang tot die markt. Eervolle vermelding, nul punten.

Jurypunten

- ✓ plausibel pad — 1 punt
- ★ plausibel én uniek — 1 punt extra
- ✕ snijpunt mét detectie — 3 punten

TOTAAL

17

Doelkaarten & scoreblad

Acht doelen op de doorlopende casus. Elk team trekt er één en ziet die van de anderen niet — dat maakt de ★-ronde spannend. Snijd langs de stippellijn; D8 hoort altijd in het spel te zitten.

CASUS

Wijkzorg-app “Naaste”

DATUM

D1 • LEZEN

Lees het dossier van één cliënt — zonder dat iemand het merkt

Je wilt weten hoe het met haar gaat en wanneer de zorg langskomt. Betrapt worden is geen optie.

WELKE ROUTES HEB JE GEDEKT?

☐ MENS

☐ TECHNIEK

☐ KETEN

WIE IS DE AANVALLER? • MOTIEF

A1 A3 A4 A5

MIN. 1 ROUTE ZONDER TECHNIEK

D2 • WIJZIGEN

Verander ongemerkt de medicatiegegevens van één cliënt

Het hoeft niet groot te zijn. Eén dosering, één dag, en niemand die het terugziet.

WELKE ROUTES HEB JE GEDEKT?

☐ MENS

☐ TECHNIEK

☐ KETEN

WIE IS DE AANVALLER? • MOTIEF

A2 A1

WIE MERKT HET, EN WANNEER?

D3 • TOEGANG

Word “mantelzorger” bij een cliënt die je niet kent

Je hoeft niets te forceren. Je hoeft alleen te worden toegelaten door iemand die je gelooft.

WELKE ROUTES HEB JE GEDEKT?

☐ MENS

☐ TECHNIEK

☐ KETEN

WIE IS DE AANVALLER? • MOTIEF

A3 A1

WIE BESLUIT DIT NU?

D4 • MISLEIDEN

Zorg dat de verzorgende vanmiddag op verkeerde informatie handelt

Niet het systeem is je doel, maar wat een mens doet met wat er op het scherm staat.

WELKE ROUTES HEB JE GEDEKT?

☐ MENS

☐ TECHNIEK

☐ KETEN

WIE IS DE AANVALLER? • MOTIEF

A2 A1

SCHADE ZONDER INBRAAK

D5 • PLATLEGGEN

Leg de app plat op het drukste moment van de dag

De vraag is niet of het lukt, maar wat mensen dán doen — en welk risico dáár ontstaat.

WELKE ROUTES HEB JE GEDEKT?

☐ MENS

☐ TECHNIEK

☐ KETEN

WIE IS DE AANVALLER? • MOTIEF

A2 A4 A6

BESCHRIJF OOK DE TERUGVAL

D6 • MEENEMEN

Neem de cliëntenlijst mee naar buiten, zonder in te breken

Je mag naar binnen. Je werkt er — of je werkte er tot vorige maand.

WELKE ROUTES HEB JE GEDEKT?

☐ MENS

☐ TECHNIEK

☐ KETEN

WIE IS DE AANVALLER? • MOTIEF

A1 A6

INSIDER: GEEN INBRAAK NODIG

D7 • UITWISSEN

Doe iets in het dossier en zorg dat niemand kan zien dat jij het was

Het gaat niet om de daad, maar om de vraag: kunnen ze het achteraf nog aan iemand koppelen?

WELKE ROUTES HEB JE GEDEKT?

☐ MENS

☐ TECHNIEK

☐ KETEN

WIE IS DE AANVALLER? • MOTIEF

A1 A4

KIJK NAAR GEDEELDE ACCOUNTS

D8 • VERTROUWEN

Beschadig het vertrouwen in de organisatie zonder één systeem aan te raken

Geen inlog, geen apparaat, geen code. Alleen mensen, verhalen en timing.

WELKE ROUTES HEB JE GEDEKT?

☐ MENS

☐ TECHNIEK

☐ KETEN

WIE IS DE AANVALLER? • MOTIEF

A6

TECHNIEK IS HIER VERBODEN

Scoreblad

Eén regel per team. De jury vult in tijdens de verdedigingsronde, hardop, met de reden erbij.

TEAM	✓	★	✕	TOTAAL

✓ 1 PT • ★ 1 PT EXTRA • ✕ 3 PT

Σ

Juryregels

1 Een pad zonder assetnummer is een mening.

Geen nummer uit het week 1-canvas, geen punt.

2 “Hoe dan?” moet in één zin kunnen.

Met een dinsdagochtend erbij: wie doet wat, waar, met wat in zijn hand.

3 Uniek is wat de zaal niet heeft.

De jury vraagt het hardop: heeft iemand anders dit ook? Eén hand omhoog en de ★ vervalt.

4 Films mogen.

Ze krijgen de eervolle vermelding en nul punten — en de vraag: voor wélke aanvaller zou dit wél kloppen?

5 Het snijpunt telt alleen mét detectie.

Een maatregel zonder “hoe merken we het” is een halve maatregel.

6 Geen echte systemen, geen echte mensen.

Alles blijft binnen de casus; dit is denkwerk op papier.

RONDE 1 • 12 MIN

Boom bouwen. Drie routes, minstens twee bladeren per route.

RONDE 2 • 8 MIN

Vellen doorgeven. Het buurtteam vult aan wat jij miste.

RONDE 3 • 15 MIN

Verdedigen. De jury vraagt bij elk blad: hoe dan?

RONDE 4 • 10 MIN

Snijpunt zoeken. Eén maatregel, zoveel mogelijk takken.

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

Minor Secure by Design • Avans Hogeschool • securebydesign.nu