

Building Block 2 – STRIDE Enumeration

Onderdeel van: Risico Analyse

Locatie in GitLab: [building-blocks/risico-analyse/stride-enumeration/](#)

Leeruitkomst: LO2 – Adviseren

Tijdsinschatting: 2 uur

Benodigheden:

- Toegang tot de **scenario's** op de DLO (zie map "scenario's")
 - STRIDE-overzicht (categorisatie van bedreigingen)
 - Hulpmiddelen voor tabellen of schema's (bijv. markdown-tabellen, Draw.io, Lucidchart)
-

Doel

In dit building block oefen je met het systematisch identificeren en categoriseren van bedreigingen met behulp van **STRIDE**. Je past STRIDE toe op een concreet scenario uit de DLO. Het resultaat vormt de basis voor het latere **risicoprofieladvies**.

Opdrachtstappen

Stap 1 – Kies een scenario

- Open de map *scenario's* in de DLO.
- Kies samen met je duo **één scenario**.
- Let op: jullie moeten **hetzelfde scenario** kiezen, maar:
 - **Iedere student werkt zijn eigen Building Block uit.**

De scenario's op de DLO zijn **summier beschreven**. Het is aan jullie om deze verder uit te werken en meer detail toe te voegen, zodat ze bruikbaar worden voor de STRIDE-analyse.

Stap 2 – Scenario uitbreiden en verhelderen

- Schrijf in 5–10 zinnen in je eigen woorden wat het scenario inhoudt.
- Breid het scenario daarna verder uit zodat het **duidelijker, overzichtelijker en rijker** wordt.
- Denk hierbij bijvoorbeeld aan:
 - Welke **actoren** spelen een rol (bijv. gebruikers, systemen of externe partijen)?
 - Welke belangrijke **middelen of gegevens** zijn betrokken (bijv. apparaten, accounts, databronnen, instellingen)?
 - Welke **uitwisseling van informatie of communicatie** vindt plaats (bijv. data die heen en weer gaat, of stappen die in het proces voorkomen)?

Dit zijn slechts voorbeelden van hoe je meer detail kunt toevoegen. Het is aan jou om het scenario zo uit te werken dat het later goed bruikbaar is voor de STRIDE-analyse.

Voorbeeld (alleen ter inspiratie, niet letterlijk overnemen): RoboMaid Vacuum

- Actoren: gebruiker, mobiele app/webinterface, cloudservice, robotstofzuiger, oplaadstation.
 - Belangrijke middelen/gegevens: schoonmaakschema's, inloggegevens, sensordata van de robot.
 - Informatiewisselingen:
 1. Robot ↔ oplaadstation (status en sensordata via RF)
 2. Oplaadstation ↔ cloud (Wi-Fi, logbestanden en instellingen)
 3. Cloud ↔ app/webinterface (inloggen, schema aanpassen, status bekijken)
-

Stap 3 – STRIDE toepassen

1. Maak een overzicht van de assets/dataflows die jij hebt geïdentificeerd.
2. Ga per asset/dataflow langs de zes STRIDE-categorieën:
 - Spoofing
 - Tampering
 - Repudiation
 - Information Disclosure
 - Denial of Service
 - Elevation of Privilege
3. Noteer per categorie of er een bedreiging denkbaar is.

4. Beschrijf kort **welke aanvalsvector** daarbij hoort.

Tip: gebruik een tabel zoals hieronder (uit te breiden naar eigen scenario):

Dataflow / Asset	S	T	R	I	D	E
Authenticatiecookie	Kan worden vervalst	Kan worden aangepast	–	–	–	–
API-verkeer	–	–	Logging kan ontbreken	Gevoelige data kan lekken	Kan worden overstroomd	–

Stap 4 – Conclusie

- Schrijf een korte samenvatting (ca. 150–200 woorden) van de belangrijkste bedreigingen in jouw scenario.
- Geef aan **welke kwetsbaarheid volgens jou het meest kritiek is**.
- Onderbouw je keuze** door uit te leggen *waarom* dit de grootste kwetsbaarheid is. Je kunt hierbij denken aan:
 - de impact op de gebruiker of organisatie;
 - de kans dat een aanval plaatsvindt;
 - de complexiteit van het misbruiken van deze kwetsbaarheid;
 - de mogelijke schade voor vertrouwelijkheid, integriteit of beschikbaarheid.

Let op: het gaat hier nog niet om een volledige risico-inschatting met kans × impact, maar je argumentatie moet wel duidelijk en onderbouwd zijn.

Inleveren

- Werk je antwoorden direct in **dit bestand** uit, onder het kopje **Antwoorden student**.
- Voeg tabellen, schema's of screenshots toe indien dat overzichtelijker is.
- Converteer dit bestand naar **PDF** met het script `pandoc_convert.py`.
- Lever in de DLO in:
 - de **PDF** (met je uitwerking, tabellen, schema's en screenshots erin);
 - eventuele losse bestanden die onderdeel zijn van je opdracht (bijv. originele schema's of afbeeldingen).

Checklist

- ☒ Scenario gekozen en kort samengevat
- ☒ Scenario uitgebreid en verhelderd (actoren, middelen/gegevens, informatiestromen)
- ☒ STRIDE toegepast per asset/dataflow
- ☒ Aanvalsvectoren beschreven
- ☒ Onderbouwde conclusie geschreven
- ☒ PDF-export gemaakt met `pandoc_convert.py`
- ☒ Bestanden ingeleverd via de DLO

Antwoorden student (vul hier je werk in)

feedback verbetering

gekregen feedback

Stap 3.3 & 3.4 For the possible threats the attack vectors are missing. Moreover, possible vulnerabilities are also not mentioned.

wat heb ik verbeterd

Ik heb stap 3 verbeterd door de attack vector bij elke Threat te zetten. en minder vaag opgeschreven ook heb ik de vulnerability duidelijk gemaakt(kwetsbaarheid).

verbeterde opdracht met gekregen feedback

Stap 3 – STRIDE-tabel

STRIDE toepassen

Dataflow / Asset	S (Spoofing)	T (Tampering)	R (Repudiation)	I (Information Disclosure)	D (Denial of Service)	E (Elevation of Privilege)
Authenticatiegegevens	Aanvalsvector: Via een Phishingsite of credential stuffing logt de aanvaller in met de gestolen gegevens als ouder. Kwetsbaarheid: Er is geen 2 factor authenticatie opgezet en hergebruik van wachtwoorden.	Aanvalsvector: Als een aanvaller of insider toegang heeft tot de database kan hij wachtwoord hashes of accounts resetten en de logins over nemen. Kwetsbaarheid: Zwakke bescherming van de database en te brede rechten	–	–	–	Aanvalsvector: Misbruik van een fout in autorisatie of in de rollen configuratie geeft de mogelijkheid een normaal account naar een beheerders account te escaleren. Kwetsbaarheid: Geen of verkeerde rolbased access control.
Wi-Fi-verbinding	Aanvalsvector: aanvaller zet een fake access point op met dezelfde SSID zodat babyfoon of ouderunit automatisch verbinden met de fake access point. Kwetsbaarheid: apparaten verifiëren het echte access point niet goed.	Aanvalsvector: Een aanvaller die op hetzelfde netwerk bezig is past onversleutelde pakketten door andere commando's mee te geven. Kwetsbaarheid: zonder end to end encryptie is er geen echte integriteitscontrole	–	Aanvalsvector: aanvaller snijft de wifi voor onversleutelde streams en kijkt mee met deze streams. Kwetsbaarheid: gebruik van onbeveiligde protocollen zoals HTTP.	Aanvalsvector: Via deauth tools of jamming verstoort de aanvaller de verbinding tussen de babyfoon en de ouderunit. Kwetsbaarheid: geen mechanisme of storingen op tevangen/ tegen te gaan.	–
Cloudstreaming	Aanvalsvector: aanvaller logt in met een nepaccount of gebruikt een gestolen sessietoken om de stream in de cloud te openen. Kwetsbaarheid: zwakke tokenbeveiliging en registratieproces.	Aanvalsvector: een man in the middle op een slecht beveiligde verbinding manipuleert videodata of commandos in de stream. Kwetsbaarheid: geen certificaat validatie.	Aanvalsvector: aanvaller misbruikt accounts of tokens terwijl acties nauwelijks worden gelogd, zodat misbruik niet herleidbaar is. Kwetsbaarheid: ontbrekende of te algemeene auditlogs.	Aanvalsvector: via slecht afgeschermd API endpoints of publieke opslag kan een aanvaller babybeelden downloaden. Kwetsbaarheid: onvoldoende toegangscontrole.	Aanvalsvector: met een DDoS op de streaming API of backend overspoelt de aanvaller de dienst zodat gebruikers geen verbinding meer krijgen. Kwetsbaarheid: geen rate limiting of DDoS mitigatie.	Aanvalsvector: via een kwetsbare admin API roept de aanvaller beheer endpoints aan om zichzelf adminrechten te geven. Kwetsbaarheid: onvoldoende authenticatie en autorisatie op beheerfuncties.

Dataflow / Asset	S (Spoofing)	T (Tampering)	R (Repudiation)	I (Information Disclosure)	D (Denial of Service)	E (Elevation of Privilege)
Gebruikersinstellingen	Aanvalsvector: Door het gebruikmaken van sessie kaping of een slecht wachtwoord logt de aanvaller in en wijzigt hij instellingen.	Aanvalsvector: De aanvaller maakt gebruik van gemanipuleerde api requests om de configuratie te wijzigen, zoals notificaties of camera's uitzetten.	Aanvalsvector: Na misbruik van een account ontkent de aanvaller zijn acties, En de configuratie wijzigingen worden niet goed gedetailleerd gelogd.	Aanvalsvector: De aanvaller leest de configuratie uit door een onbeveiligd configuratie bestand of configuratie endpoint.	–	–
	Kwetsbaarheid: Het gebruik van zwakke wachtwoorden, geen gebruik maken van 2 stappen verificatie en onvoldoende bescherming van de sessies.	Kwetsbaarheid: geen serverside autorisatie en input controles	Kwetsbaarheid: geen goede logging van de instellingen.	Kwetsbaarheid: gevoelige gegevens beschikbaar in een text bestand of een open configuratie api		
Cloudbeheeromgeving	Aanvalsvector: Via een gerichte Phishing attack(spear phishing) verkrijgt een aanvaller de inloggegevens van een medewerker en logt hij in op de cloudbeheer console	Aanvalsvector: Aanvaller of insider bemachtigd beheersrechten en wijzigt of wist logs en of klantdata in de database om sporen te wissen.	–	Aanvalsvector: Een beheerder kan zonder enige beperkingen klant date overzien en exporteren.	–	Aanvalsvector: Insider misbruikt een foutje om zijn rol op te hogen naar admin.
	Kwetsbaarheid: Weinig bescherming tegen phishing(security awareness) en geen authenticatie.	Kwetsbaarheid: geen integriteits controle op logs en te breede rechten.		Kwetsbaarheid: te breede toegang in beheerders dashboard.		Kwetsbaarheid: Een te zwakke schijding tussen rollen zonder extra controles bij een rolwijziging

Stap 1 – Scenario

Ik heb gekozen samen met Xavier Rijs voor p6 SkyBaby Monitor De SkyBaby Monitor is ontworpen om ouders te helpen hun kind gemakkelijk in de gaten te houden via een draadloos camerasysteem en een bijbehorende kijk- en bedieningsunit.

De SkyBaby Monitor bestaat uit een camera-unit voor in de kinderkamer, een speciale ouderunit, en een smartphone-applicatie. De camera is uitgerust met nachtzicht en een microfoon. De ouderunit heeft een scherm voor live videoweergave, een speaker, en een spreek-knop om met de baby te communiceren.

De camera-unit staat via Wi-Fi rechtstreeks in contact met de ouderunit. Zodra de camera beweging of geluid detecteert, stuurt hij een signaal naar de ouderunit, die het beeld en geluid in realtime weergeeft. Als gebruikers de optionele cloudkoppeling activeren, kan de camera de videobeelden ook naar een online portal sturen. In dit geval kan de gebruiker via de smartphone-app of een webbrowser op afstand worden meekijken en instellingen (zoals de geluidsgevoeligheid of de helderheid van de camera) aanpassen.

Stap 2 – Uitbreiding en verheldering

De SkyBaby Monitor is een slim babybewakingssysteem dat ouders in staat stelt hun kind op afstand te bekijken en te beluisteren. Het systeem bestaat uit een camera-unit in de babykamer, een ouderunit met scherm en speaker, en een smartphone-app met cloudfunctionaliteit voor toegang op afstand. De opdrachtgever is een fabrikant van slimme huisapparaten die betrouwbare en veilige babybewakingsproducten op de markt wil brengen. De doelgroep bestaat uit ouders met jonge kinderen die waarde hechten aan gemak, veiligheid en gemoedsrust

Actoren

Actor	Beschrijving	Rol in het proces
Ouder / Gebruiker	De persoon die de SkyBaby Monitor gebruikt om het kind te bekijken en instellingen te beheren.	Start verbindingen, bekijkt videobeelden en ontvangt meldingen.
Camera-unit (SkyBaby Cam)	Slim apparaat met camera, microfoon en Wi-Fi-module in de babykamer.	Legt beelden vast en stuurt data via Wi-Fi of de cloud.
Ouderunit (handheld)	Apparaat met scherm en speaker.	Toont live beelden en audio, ontvangt meldingen.
Smartphone-app / Webapp	Software voor beheer en afstandsbediening.	Zorgt voor inloggen, instellingen, en cloudcommunicatie.
SkyBaby Cloudserver	Online dienst die data verwerkt en opslag en authenticatie regelt.	Verwerkt streaming, opslag en accountbeheer.
Netwerk (Wi-Fi / Internet)	Verbindingskanaal tussen apparaten.	Transporteert videodata en meldingen.
Beheerder / Insider	Medewerker die toegang heeft tot cloudbeheer of onderhoud uitvoert.	Beheert accounts, servers en logging.

Belangrijke middelen of gegevens

Middel / Gegeven	Beschrijving	Belang
Videobeelden	Live en opgeslagen video van de babykamer.	Zeer privacygevoelig, kern van de dienst.
Inloggegevens	Gebruikersnaam, wachtwoord, authenticatietokens.	Noodzakelijk voor toegang en beveiliging.
Instellingen	Configuratie van camera en app.	Beïnvloedt werking en veiligheid.
Clouddatabase	Slaat accounts, logs en instellingen op.	Cruciaal voor continuïteit en beheer.
Firmware / App-code	Software die de apparaten aanstuurt.	Kan kwetsbaarheden bevatten.
Communicatiekanalen	Wi-Fi, HTTPS en API-verbindingen.	Bevatten gevoelige data, moeten veilig zijn.

Informatie-uitwisseling / Communicatie

Stap	Beschrijving van communicatie	Betrokken partijen	Gegevens of middelen
1. Installatie	De gebruiker koppelt de camera aan het Wi-Fi-netwerk via de app.	Gebruiker, Camera, Cloud	Wi-Fi- en accountgegevens
2. Authenticatie	App of ouderunit logt in op de cloudserver om verbinding te maken.	App, Cloudserver	Gebruikersnaam, wachtwoord, token
3. Lokale streaming	Camera stuurt livebeelden direct via Wi-Fi naar de ouderunit.	Camera, Ouderunit	Real-time video en audio
4. Cloudstreaming	Camera streamt beelden naar cloud, gebruiker bekijkt via app.	Camera, Cloud, App	Geëncrypteerde videodata
5. Meldingen	Camera detecteert beweging/geluid en stuurt notificaties.	Camera, App, Cloud	Bewegingsdata, timestamps
6. Instellingswijziging	Gebruiker past instellingen aan via app, doorgegeven aan camera.	Gebruiker, Cloud, Camera	Configuratiedata
7. Logging & beheer	Cloud logt alle toegang, updates en systeemfouten.	Cloud, Beheerder	Gebruikersactiviteit, systeemlogs

Stap 3 – STRIDE-tabel**STRIDE toepassen**

Dataflow / Asset	S (Spoofing)	T (Tampering)	R (Repudiation)	I (Information Disclosure)	D (Denial of Service)	E (Elevation of Privilege)
------------------	--------------	---------------	-----------------	----------------------------	-----------------------	----------------------------

Dataflow / Asset	S (Spoofing)	T (Tampering)	R (Repudiation)	I (Information Disclosure)	D (Denial of Service)	E (Elevation of Privilege)
Authenticatiegegevens	Aanvalsvector: Via een Phishingsite of credential stuffing logt de aanvaller in met de gestolen gegevens als ouder. Kwetsbaarheid: Er is geen 2 factor authenticatie opgezet en hergebruik van wachtwoorden.	Aanvalsvector: Als een aanvaller of insider toegang heeft tot de database kan hij wachtwoord hashes of accounts resetten en de logins over nemen. Kwetsbaarheid: Zwakke bescherming van de database en te brede rechten	–	–	–	Aanvalsvector: Misbruik van een fout in autorisatie of in de rollen configuratie geeft de mogelijkheid een normaal account naar een beheerders account te escaleren. Kwetsbaarheid: Geen of verkeerde rolbased access control.
Wi-Fi-verbinding	Aanvalsvector: aanvaller zet een fake access point op met dezelfde SSID zodat babyfoon of ouderunit automatisch verbinden met de fake access point. Kwetsbaarheid: apparaten verifiëren het echte access point niet goed.	Aanvalsvector: Een aanvaller die op hetzelfde netwerk bezig is past onversleutelde pakketten door andere commando's mee te geven. Kwetsbaarheid: zonder end to end encryptie is er geen echte integriteitscontrole	–	Aanvalsvector: aanvaller snijft de wifi voor onversleutelde streams en kijkt mee met deze streams. Kwetsbaarheid: gebruik van onbeveiligde protocollen zoals HTTP.	Aanvalsvector: Via deauth tools of jamming verstoort de aanvaller de verbinding tussen de babyfoon en de ouderunit. Kwetsbaarheid: geen mechanisme of storingen op tevangen/ tegen te gaan.	–
Cloudstreaming	Aanvalsvector: aanvaller logt in met een nepaccount of gebruikt een gestolen sessietoken om de stream in de cloud te openen. Kwetsbaarheid: zwakke tokenbeveiliging en registratieproces.	Aanvalsvector: een man in the middle op een slecht beveiligde verbinding manipuleert videodata of commandos in de stream. Kwetsbaarheid: geen certificaat validatie.	Aanvalsvector: aanvaller misbruikt accounts of tokens terwijl acties nauwelijks worden gelogd, zodat misbruik niet herleidbaar is. Kwetsbaarheid: ontbrekende of te algemeene auditlogs.	Aanvalsvector: via slecht afgeschermd API endpoints of publieke opslag kan een aanvaller babybeelden downloaden. Kwetsbaarheid: onvoldoende toegangscontrole.	Aanvalsvector: met een DDoS op de streaming API of backend overspoelt de aanvaller de dienst zodat gebruikers geen verbinding meer krijgen. Kwetsbaarheid: geen rate limiting of DDoS mitigatie.	Aanvalsvector: via een kwetsbare admin API roept de aanvaller beheer endpoints aan om zichzelf adminrechten te geven. Kwetsbaarheid: onvoldoende authenticatie en autorisatie op beheerfuncties.

Dataflow / Asset	S (Spoofing)	T (Tampering)	R (Repudiation)	I (Information Disclosure)	D (Denial of Service)	E (Elevation of Privilege)
Gebruikersinstellingen	Aanvalsvector: Door het gebruikmaken van sessie kaping of een slecht wachtwoord logt de aanvaller in en wijzigt hij instellingen.	Aanvalsvector: De aanvaller maakt gebruik van gemanipuleerde api requests om de configuratie te wijzigen, zoals notificaties of camera's uitzetten.	Aanvalsvector: Na misbruik van een account ontkent de aanvaller zijn acties, En de configuratie wijzigingen worden niet goed gedetailleerd gelogd.	Aanvalsvector: De aanvaller leest de configuratie uit door een onbeveiligd configuratie bestand of configuratie endpoint.	–	–
	Kwetsbaarheid: Het gebruik van zwakke wachtwoorden, geen gebruik maken van 2 stappen verificatie en onvoldoende bescherming van de sessies.	Kwetsbaarheid: geen serverside autorisatie en input controles	Kwetsbaarheid: geen goede logging van de instellingen.	Kwetsbaarheid: gevoelige gegevens beschikbaar in een text bestand of een open configuratie api		
Cloudbeheeromgeving	Aanvalsvector: Via een gerichte Phishing attack(spear phishing) verkrijgt een aanvaller de inloggegevens van een medewerker en logt hij in op de cloudbeheer console	Aanvalsvector: Aanvaller of insider bemachtigd beheersrechten en wijzigt of wist logs en of klantdata in de database om sporen te wissen.	–	Aanvalsvector: Een beheerder kan zonder enige beperkingen klant data overzien en exporteren.	–	Aanvalsvector: Insider misbruikt een foutje om zijn rol op te hogen naar admin.
	Kwetsbaarheid: Weinig bescherming tegen phishing(security awareness) en geen authenticatie.	Kwetsbaarheid: geen integriteits controle op logs en te breede rechten.		Kwetsbaarheid: te breede toegang in beheerders dashboard.		Kwetsbaarheid: Een te zwakke schijding tussen rollen zonder extra controles bij een rolwijziging

Stap 4 – Conclusie

In de STRIDE-analyse kunnen we concluderen dat de SkyBaby Monitor Kwetsbaar is op het gebied van authenticatie, gegevenslekken en privilege-escalatie. Een groot deel van het risico komt door de cloudstream en de authenticatieprocessen omdat dit gevoelige gebruikersdata en videobeelden bevat.

De meest kritieke bedreiging is Information Disclosure via de cloudomgeving. Een lek van babybeelden heeft een directe impact op de vertrouwelijkheid en kan leiden tot reputatieschade en verlies van klantvertrouwen.

De kans is bovendien realistisch, omdat apparaten zoals babycamera's vaak doelwit zijn van datalekken of slechte configuraties.

Een succesvolle aanval zou ernstige privacyproblemen veroorzaken en mogelijk juridische gevolgen hebben onder de AVG.