Procesvoorstel ten aanzien van apps vanuit NV

Doel

Dit document heeft tot doel het verkenningsproces ten aanzien van de ontwikkeling van apps i.r.t. COVID-19 te ondersteunen vanuit het perspectief van cybersecurity en nationale veiligheid. Vanuit dit perspectief adviseren NCTV, NCSC en AIVD de volgende noties mee te nemen in het vervolgtraject.

Samenvatting

- Werk de businesscase uit;[1]
- Betrek partijen als de GGD, de ontwikkelaar en een security architect vanaf het begin in de discussie rondom de functionaliteit en beveiligingsrisico's van de app;
- Alleen met een concreet beeld rondom de businesscase en functionaliteiten als startpunt is een effectieve beveiligingsdiscussie mogelijk;
- Volg voor een juiste afweging van beveiligingsrisico's het hierna geschetste stappenplan;
- Verzorg de hierna geschetste benodigdheden voor een effectieve afweging van beveiligingsrisico's.

Inhoud

[1] Een businesscase of een haalbaarheidsstudie is een projectmanagement-term waarin de zakelijke afweging om een project of taak te beginnen beschreven wordt. In de businesscase worden de kosten tegen de baten afgewogen, rekening houdend met de risico's.

Aanleiding

Op 23 april jl. hebben NCTV, NCSC en AIVD gesproken met (10)(2e), project-/programmamanager binnen de Directie Informatiebeleid van VWS. Doel van het gesprek was om beter zicht te krijgen op het proces ten aanzien van de ontwikkeling van apps i.r.t. COVID-19. Op dit moment werkt VWS aan een vervolgaanpak en -proces. VWS komt eind april bij genoemde partijen op de lijn over het vervolg. In het gesprek hebben we aan de hand van de 5G-aanpak toegelicht hoe een dergelijk proces eruit kan zien, welke elementen erin zouden moeten zitten, welke randvoorwaarden er ingevuld moeten worden en hoe onze bijdrage eruit kan zien. Dit is, gelet op de huidige gedachtevorming binnen VWS, op een redelijk abstract niveau beschreven. Het ontwikkelen van een app is één van de mogelijke scenario's om de GGD te ontlasten en/of de werkwijze efficiënter te maken bij het doen van grootschalig contactonderzoek.

Hieronder zetten wij een werkwijze uiteen ter ondersteuning van het proces om de mogelijkheden van verschillende apps te onderzoeken t.b.v. de ondersteuning van de GGD en hoe deze apps aan nationale veiligheidsaspecten getoetst kunnen worden. Dit zullen we doen aan de hand van onze observaties van de afgelopen weken, alvorens hier nader op in te gaan.

Terugkijkend

Als we kijken naar de afgelopen weken zien wij o.a. veel onduidelijkheid over:

- het proces om te komen tot de app(s);
- de businesscase achter de app(s);
- de functionele eisen t.a.v. de app(s);
- en de manier waarop de app(s) technische invulling krijgt/krijgen.

Dit heeft geleid tot een zeer brede en ongestructureerde discussie die om die reden maar beperkt effectief was.

Wij willen hieronder enkele gedachten delen waar het gaat om het aanbrengen van structuur in de discussie en het omgaan of wegnemen van de onduidelijkheden.

Businesscase en functionaliteit

De behoefte om een app te bouwen komt voort uit een bepaalde behoefte en/of een bepaald probleem dat ingevuld/opgelost dient te worden. Een app is een mogelijk middel om (deels) in deze behoefte te kunnen voorzien of om het probleem op te lossen. Afhankelijk van de door de app geboden functionaliteiten en de technische invulling zal deze er in meer of mindere mate in slagen om in deze behoefte te voorzien dan wel een (deel)oplossing te bieden voor het probleem. Uitgangspunt hierbij is dat het helder moet zijn welk overkoepelend probleem opgelost moet worden.

Meer functionaliteit in een app betekent echter veelal een groot aanvalsoppervlak en daardoor meer risico's die beheerst dienen te worden. Als het niet lukt om de risico's voldoende te beheersen, kan ervoor worden gekozen de functionaliteiten van de app te beperken. Naarmate functionaliteit van de app verder beperkt wordt, heeft dat consequenties voor de effectiviteit van de app. Hierdoor is er dan mogelijk geen positieve businesscase meer voor de app te maken.

Om de juiste balans hierin te vinden, menen wij dat het verstandig is om partijen als de GGD, de ontwikkelaar en een security architect vanaf het begin nauw te betrekken in de discussie rondom de functionaliteit en beveiligingsrisico's van de app.

Structuur in de beveiligingsdiscussie

Het startpunt van de beveiligingsdiscussie is een concreet beeld rondom de businesscase en functionaliteiten van de app. Zonder dit startpunt is een effectieve beveiligingsdiscussie naar onze mening niet mogelijk.

Om ervoor te zorgen dat de beveiligingsdiscussie zich richt op de meest relevante risico's stellen wij het volgende gestructureerde stappenplan voor, dat ook gehanteerd is in het 5G-risicoafwegingsproces, dat vorig jaar door NCTV, NCSC, Agentschap Telecom en AIVD/NBV is doorlopen.

1. Uitvoeren van een dreigingsanalyse (hierbij wordt informatie uit open bronnen en dreigingsinformatie vanuit de AIVD gebruikt)
2. Bepalen van de te beschermen belangen (in samenspraak met o.a. VWS en GGD)
3. Vaststellen van de meest relevante risico's (deze zullen op basis van input van de experts vanuit cybersecurity en nationale veiligheidsveld (hierna: NV) samen met VWS en GGD worden geformuleerd).
4. Bepalen van mogelijke maatregelen om de meest relevante risico's te beheersen (deze zullen op basis van input de experts vanuit NV samen met VWS en GGD worden geformuleerd).
5. Omdat risico's niet tot nul terug te brengen zijn, adviseren wij om aan het einde van het proces ook een concreet plan uit te werken waar het gaat om het handelen na een eventueel succesvolle aanval (*incident response readiness*).

In onderstaand stroomschema is in de basis weergegeven hoe een dergelijk afwegingsproces eruit kan zien.

Dreigingsanalyse

Inzicht in de dreiging is essentieel voor het maken van een risico-inschatting. NCTV, NCSC en AIVD kunnen VWS helpen bij het komen tot een algeheel dreigingsbeeld.

Bij het maken van een dreigingsanalyse worden op hoofdlijnen de volgende vragen beantwoord:

- Vanuit welke actoren gaat een dreiging uit?
- Wat is hun intentie?
- Hebben zij de potentie om te komen tot (geavanceerde) aanvallen?
- Wat is er bekend over de verschillende manieren van handelen (modus operandi)?

Door het beantwoorden van dergelijke vragen, kan worden bepaald in welke mate er rekening gehouden dient te worden met bepaalde actoren waar dreiging vanuit gaat.

Te beschermen belangen

Voordat er concreet gediscussieerd kan worden over risico's en beveiliging van de app, moeten de te beschermen belangen (tbb's) in relatie tot de app duidelijk worden gemaakt. Daarnaast moet de relevantie en prioritering van deze tbb's worden bepaald (*zijn bepaalde tbb's belangrijker dan andere?*).

Ook moet een inschatting worden gemaakt in welke mate groepen waar dreiging vanuit gaat, interesse hebben in deze specifieke tbb's.

Als laatste moet er worden bepaald hoe de meest relevante tbb's te relateren zijn aan de technische oplossingen die voorliggen. Hiervoor is een beeld van het systeemlandschap (technische / beveiligingsinfrastructuur) nodig.

Hieronder volgen enkele voorbeeldvragen, die kunnen helpen bij het concreet maken van het beeld rondom de tbb's:

- Wat gaat er fout als deze informatie in de verkeerde handen valt?
- Hoe erg is dat eigenlijk (van reputatieschade tot en met het gevaar voor mensenlevens)?
- Wat gaat er fout als gegevens gemanipuleerd worden en hoe erg is dat?
- Hoe belangrijk is het dat de systemen/de informatie te allen tijde beschikbaar is/zijn?
- Gaat het hier om de vertrouwelijkheid of misschien meer over integriteit of beschikbaarheid van informatie?
- Waar bevindt deze informatie zich in ons IT-landschap?
- Gaat het om een grote dataverzameling of betreft het slechts vluchtige gegevens?
- Welke systemen zijn er betrokken bij de verwerking van deze gegevens?
- Waar kan een aanvaller mogelijk digitale sporen van deze informatie vinden?

Identificeren van de meest voorstelbare risico's

Op basis van de dreigingsanalyse (kans) en het overzicht aan tbb's (impact) kunnen vervolgens de risico's worden geconcretiseerd en gescoord op relevantie.

Het bedenken van risico's is veelal een creatief proces waarbij meerdere disciplines aanwezig zijn. Het gaat hierbij om zowel technici als mensen die de business vertegenwoordigen. Modellen als de *Cyber kill chain* en het *ATT&CK framework* kunnen helpen bij deze fase.

In het geval er meerdere technische oplossingen op tafel liggen, moeten de risico's per oplossing worden geïdentificeerd.

Op basis van de dreigingsinschatting en het scoren van de tbb's is het mogelijk om aan het einde van deze stap op hoofdlijnen een geprioriteerd overzicht van de meest relevante risico's per technische oplossing op te stellen.

Bepalen gerichte maatregelen

Aan de hand van het geprioriteerde overzicht van de meest voorstelbare risico's kan er worden gedacht aan maatregelen om deze risico's te beheersen tot een acceptabel niveau. Dit kunnen zowel technische als niet technische maatregelen zijn.

Daarnaast kunnen deze maatregelen zich richten op het voorkomen van een risico (preventief) of zich richten op het beperken van het negatief effect dat een risico heeft, indien deze werkelijkheid wordt (repressief).

Het is mogelijk dat men aan het einde van deze stap tot de conclusie komt dat de risico's in de technisch oplossingen onvoldoende te beheersen zijn. Indien deze restrisico's niet te accepteren zijn, staat men voor de keuze om eventueel de functionaliteit van de app te beperken, zodat deze risico's afvallen. In een dergelijk geval moet opnieuw worden getoetst of er na het beperken van de functionaliteit alsnog een positieve businesscase overblijft.

Als de risico's voldoende te beperken en de restrisico's te accepteren zijn, adviseren wij om de laatste stap in het proces te zetten. Dit is het uitwerken van een incidentproces.

Incidentproces

Het is erg onwaarschijnlijk dat alle risico's volledig te beheersen zijn. Er zullen in bepaalde mate – afhankelijk van de risicobereidheid – restrisico's overblijven. Het is daarom van groot belang dat er een plan is hoe te handelen indien een van de risicoscenario's realiteit wordt.

Er zijn verschillende elementen, die in een dergelijk plan uitgewerkt dienen te worden. Denk hierbij aan communicatie, verantwoordelijkheden, mandaten, bereikbaarheid en ondersteuning.

Hieronder zijn enkele voorbeelden van vragen opgesomd die kunnen helpen bij het concreet maken van deze laatste stap.

- Welke partijen kunnen ons ondersteunen tijdens een incident?
- Hoe communiceren wij op een veilige manier tijdens een incident?
- Wie is verantwoordelijk voor het nemen van impactvolle beslissingen zoals het uitzetten van systemen?
- Zijn systemen voldoende voorbereid op het uitvoeren van digitaal forensisch onderzoek n.a.v. een incident (bv. logging)?

Rol nationale veiligheid in het proces

Binnen het proces kunnen NCTV, NCSC en AIVD als volgt bijdragen:

- Vanuit nationale veiligheid adviseren over het proces om te komen tot een gewogen afweging op basis van dreigingen en risico's
- Expertise op risicomanagement proces
- Expertise op het gebied van dreiging
- Expertise op het gebied van technische oplossingen
- Expertise op crypto
- Expertise op het gebied van nationale veiligheid

Benodigdheden voor de beveiligingsdiscussie

Om het beschreven proces en de discussie te faciliteren is het wenselijk om bepaalde documentatie, minimaal op hoofdlijnen, gedurende het proces beschikbaar te hebben. Denk hierbij aan:

- Beschrijving business case
- Technische security documentatie
    - High-level design
    - Low-level design
    - Security architectuur
- Functioneel ontwerp
- Data lifecycle management diagram