Wat moet de overheid doen op het gebied van cybersecurity?

Renato Kuiper (6 maart 2020)

Het meest belangrijke bij de overheid is dat ze:

1. Risicomanagement gaan invoeren, en in geval van security dit ook op cyber security gebied. Ze roepen het vaak in allerlei beleidsstukken, en in zaken als de BIR[1] en BIO[2], maar doen het vaak niet.
2. Baselines als de BIO met een niet logische basisbeveiligingsniveau (BBN), aanpassen zodat ze werkbaar worden. Kwaliteitsaspecten zoals integriteit, beschikbaarheid en vertrouwelijkheid horen hand in hand met elkaar op te gaan. Met andere woorden: als een informatiesysteem een hoge beschikbaarheid heeft (BBN3), dan zijn de integriteit en vertrouwelijkheid eveneens hoog. Bij een publieke website van de overheid geldt dat voor de beschikbaarheid en integriteit wel, maar de vertrouwelijkheid is absoluut niet hoog maar openbaar. Met andere woorden heroverweeg die BBN niveaus.
3. Security in architectuur borgen, en daar bij de uitvoering ook op toetsen. Hierbij vervult de security architectuur de rol van het vertalen van het informatiebeveiligingsbeleid naar concrete maatregelen in techniek, organisatie en processen. De security architectuur creëert dan overzicht, inzicht en samenhang van het stelsel van informatiebeveiligingsmaatregelen. Op basis van een inventarisatie van de huidige situatie, kan middels de security architectuur (toekomstige en gewenste situatie) het verschil bepaald worden en vervolgens kan deze in de roadmap voor realisatie worden geplaatst. Bij projecten die binnen de overheid gestart worden kan de security architectuur de securityprincipes en -richtlijnen meegeven in de PSA[3]. Tijdens de uitvoering van het project kunnen de security architecten meehelpen deze principes en richtlijnen toe te passen en aan het einde van het project te toetsen op de realisatie daarvan.
4. Per ministerie en uitvoeringsorganisatie bewust nadenken over de risicostrategie, en een duidelijke ‘risk appetite’ (risicobereidheid) formuleren. De risicostrategie kan zijn: risico-mijdend (wat je nu veel binnen de overheid ziet), risico-nemend (meer ondernemerschap) of risico-neutraal (balans zoeken). Maar laten ze vooral bepalen welk risico’s ze bewust willen nemen (de risk appetite)!

Pas als deze vier punten goed ingeregeld zijn, kun je de concrete maatregelen voor security vormgeven en daar ook op sturen.

---

[1] De BIR is een gemeenschappelijk normenkader voor de beveiliging van de informatie(systemen). De BIR 2017 is volledig gebaseerd op de internationale norm ISO/IEC 27002. Het concretiseert een aantal eisen tot verplichte operationele afspraken (rijksmaatregelen), om een eenduidig minimumniveau van beveiliging voor gegevens te garanderen. De standaard basisbeveiligingsniveaus (BBN's) met bijbehorende beveiligingseisen maken risicomanagement eenvoudiger.

[2] Vanaf 1 januari 2020 is de Baseline Informatiebeveiliging Overheid (BIO) van kracht. De BIO vervangt de bestaande baselines informatieveiligheid voor Gemeenten, Rijk, Waterschappen en Provincies. Van BIG, BIR, BIR2017, IBI en BIWA naar BIO. Hiermee ontstaat één gezamenlijk normenkader voor informatiebeveiliging binnen de gehele overheid, gebaseerd op de internationaal erkende en actuele ISO-normatiek.

[3] PSA is de afkorting van Project Start Architectuur, een document dat de kwaliteitseisen en de oplossingsrichting aangeeft voor een project.