10 Security by Design: een nieuw modewoord of hét toverwoord in de strijd tegen cybercrime?

Natascha van Duuren

Cyberaanvallen en datalekken staan bovenaan de lijst met risico's die bestuurders het meeste zorgen baren. Dit is niet zonder reden. Datalekken zijn aan de orde van de dag en cyberaanvallen nemen steeds meer toe. "Privacy by Design", "Privacy by Default" en "Security by Design" zijn begrippen die in dit kader vaak worden gebruikt. Wat betekenen deze begrippen precies en wat betekenen deze begrippen concreet voor organisaties en bedrijven? En, last but not least, is Security by Design de oplossing voor onze (terechte) zorgen met betrekking tot cybercrime? Een korte uiteenzetting.

Eerste introductie Privacy by Design

Het begrip Privacy by Design is in de jaren '90 geïntroduceerd door Canadese privacy toezichthouder Ann Cavoukian. Het begrip 'privacy-enhancing technologies (PETs)' bestond al. Ann Cavoukian was van mening dat "*a more substantial approach" vereist* is. Met andere woorden, niet alleen technische, maar ook organisatorische en fysieke maatregelen.

Ann Couvakian introduceerde de '7 foundational principles':

- Proactief in plaats van reactief – preventief in plaats van herstellend
- Privacy als standaard
- Privacy geïntegreerd in het ontwerp
- Volledige functionaliteit – 'positive sum' in plaats van 'zero-sum'
- Veiligheid van begin tot eind – bescherming tijdens de volledige levenscyclus
- Zichtbaarheid en transparantie – houd het open
- Respect voor de privacy – laat de gebruiker centraal staan

Met de 7 beginselen van Privacy by Design, werd in feite ook Privacy by Default geïntroduceerd (in de vorm van het beginsel 'Privacy als standaard') en Security by Design (in de vorm van het beginsel 'Veiligheid van begin tot eind, bescherming tijdens de volledige levenscyclus'). Krachtige veiligheidsmaatregelen van begin tot eind zijn volgens Ann Cavoukian essentieel voor het behoud van privacy.

Implementatie van Privacy by Design in onze wet- en regelgeving

De opvatting van Ann Cavoukian heeft navolging gekregen. Inmiddels zijn de beginselen van Privacy by Design gecodificeerd.

Zo leggen onze Algemene Verordening Gegevensbescherming (AVG) Privacy by Design (artikel 25 lid 1 AVG) en Privacy by Default (artikel 25 lid 2 AVG) als verplichting op, ook al worden deze termen niet expliciet genoemd. In de literatuur zijn opmerkingen gemaakt over het abstracte karakter van artikel 25 AVG. Zo zijn er geluiden dat de eisen die in dit artikel zijn opgenomen, het midden houden tussen een abstract geformuleerd beginsel en een min of meer concrete opdracht.[187]

Deze kritiek is mijns inziens terecht. Goed beschouwd noemt artikel 25 lid 1 AVG slechts twee concrete verplichtingen:

- Dataminimalisatie (zie ook artikel 5 lid 1 sub c AVG): alleen strikt noodzakelijke gegevens verzamelen
- Pseudominiseren (zie ook artikel 4 lid 5 AVG

Verder bevat de AVG een aantal afzonderlijke bepalingen met verplichtingen die nauw samenhangen met Privacy by Design & Default. Je kunt het ook anders stellen: om te kunnen voldoen aan deze verplichtingen is het noodzakelijk Privacy by Design toe te passen:

- Encryptie (art 6 lid 4 sub e, art. 32 lid 1 sub a AVG)
- Bewaren (art. 5 lid 1 sub e AVG)

Uitleg in de praktijk

De vraag is: Hoe moeten deze (deels abstracte) verplichtingen in de praktijk worden uitgevoerd? Welk houvast hebben bedrijven en organisaties daarbij?

In 2015, al voor invoering van de AVG, heeft ENISA[188] in haar rapport '*Privacy and Data Protection by Design – from policy to engineering*'[189] getracht een brug te bouwen tussen '*the legal framework*' en '*the available technologies implementation measures*'. Vier jaar later heeft de EDPD[190] richtlijnen[191] gepubliceerd over de toepassing van *data protection by design en default*. Ondanks de goedbedoelde pogingen bieden de richtlijnen niet het houvast die zij beoogden te bieden. Bestudering van de richtlijnen leidt mijns inziens tot de conclusie dat slechts een aantal voorbeelden en handvatten wordt gegeven, maar dat de richtlijnen toch vrij abstract blijven. Hetzelfde geldt voor het eerder verschenen ENISA-rapport.

187 Zie bijvoorbeeld H.J. Bolte in 'EDPB richtlijnen over Data Protection by Design en Default' in Privacy & Informatie (P&I),

188 European Union Agency for Cybersecurity

189 https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design

190 European Data Protection Board

191 Guidelines 4/2019 on Article 25 Data Protection by Design and Default

ENISA is deze mening overigens ook zelf aangedaan. In haar rapport '*Guidance and gaps analysis for European Standardisation*'[192] komt zij onder meer tot de volgende bevindingen:

- Het concept van privacy-by-design en de implementatie ervan worden nog steeds niet duidelijk gepresenteerd, ondanks een algemene consensus over waargenomen voordelen;
- Het aantonen van naleving van privacynormen op het gebied van informatiebeveiliging is niet zo eenvoudig als verwacht. Sommige benaderingen voor conformiteitsbeoordeling zijn beschikbaar in specifieke sectoren, andere ontberen nog steeds passende mechanismen;
- Een coherente analyse van sectorspecifieke behoeften aan privacystandaardisatie is essentieel, vooral in de context van informatiebeveiliging;
- Er is een toenemende behoefte om het in kaart brengen van internationale normen en Europese regelgevingsvereisten en te analyseren, aangezien verwijzingen naar normen in de EU-wetgeving steeds vaker voorkomen en er aanzienlijke verschillen zijn met rechtsgebieden buiten de EU.

ENISA snijdt met deze laatste bevinding een belangrijk punt aan. Privacy- en cybersecuritynormen zullen op Europees niveau moeten worden ontwikkeld en niet uitsluitend op het niveau van een individueel land.

Security by Design en de Nederlandse overheid

Een interessante vraag in dit kader is: hoe gaat de Nederlandse overheid met Privacy by Design omgaat, meer specifiek met Security by Design? Digitale veiligheid is immers onlosmakelijk verbonden met de nationale veiligheid. Het belang van Security by Design bij overheidsautomatisering staat buiten kijf en werd onlangs nog eens onderstreept toen een datalek in de systemen van de GGD werd geconstateerd. In de Kamerbrief van Staatssecretaris Knops van BZK naar aanleiding van de motie Kröger c.s., wordt 'Privacy by design' expliciet genoemd, evenals de 7 principes van Ann Cavoukian. In de brief wordt gerefereerd aan de overheidsbrede maatregelen die reeds zijn getroffen, waaronder het instrument Inkoopeisen Cybersecurity Overheid (ICO). Tegelijkertijd geeft de Staatssecretaris aan dat deze maatregelen verder aangevuld dienen te worden vanuit de zeven principes.[193] Ook in het Cybersecuritybeeld Nederland 2021[194] van het NCTV[195] en het NCSC[196] wordt expliciet benoemd

192 https://www.enisa.europa.eu/publications/guidance-and-gaps-analysis-for-european-standardisation
193 De verwachting is dat deze invulling in de loop van 2021 gereed is.
194 https://www.nctv.nl/documenten/publicaties/2021/06/28/cybersecuritybeeld-nederland-2021
195 Nationaal Coördinator Terrorismebestrijding en Veiligheid
196 Nationaal Cyber Security Centrum

dat een baseline[197] niet voldoende is en wordt de noodzaak van nadere regulering erkend.

Verantwoordelijkheid voor Security by Design

Ervan uitgaande dat het Europees en Nederlands voornemen om Privacy (en daarmee Security) by Design nadere invulling te geven daadwerkelijk wordt gerealiseerd, is het de vraag wie verantwoordelijk is voor de juiste toepassing daarvan. Op grond van de AVG is Privacy & Security by Design een verplichting van de verwerkingsverantwoordelijke (in veel gevallen de opdrachtgever). De praktijk is echter, dat verwerkingsverantwoordelijken software niet zelf ontwikkelen en dat door de opdrachtgever vaak te weinig eisen worden gesteld ten aanzien van beveiliging. Dit heeft tot gevolg dat kwetsbaarheden in de software vaak pas aan het licht komen in de gebruiksfase, soms pas op het moment dat er een cyberincident plaatsvindt. Dit is uiteraard een onwenselijke zaak.

Het zou daarom goed zijn als de verplichting van Security by Design zich ook rechtstreeks zou richten tot developers en aanbieders. Met name bij standaardsoftware zou het mijns inziens zo moeten zijn dat een afnemer erop zou moeten kunnen vertrouwen dat bij de ontwikkeling van de software Security by Design is toegepast: Veiligheid van begin tot eind, bescherming tijdens de volledige levenscyclus (waarbij geldt dat de toepassing en het gebruik van standaardsoftware eveneens bepalend zijn voor de veiligheid en deze factoren uiteraard buiten de invloedsfeer en verantwoordelijkheid van de developers en aanbieders liggen). Daarbij komen we wel weer terug op een eerder punt, te weten dat eerst op Europees niveau nadere invulling zal moeten worden gegeven aan de verplichtingen die Security by Design met zich meebrengt. (Om het niet nog complexer en enigszins behapbaar te houden laten we het mondiale karakter van digitalisering vooralsnog buiten beschouwing).

Conclusie

Security by Design is geen nieuw modewoord. Het bestaat al sinds de jaren '90 en in inmiddels gecodificeerd. Het belang van Security by Design als onderdeel van Privacy by Design in de strijd tegen cybercrime staat buiten kijf. Het ontbreken van een definitie en concrete invulling van Security by Design op Nederlands en Europees niveau heeft echter tot gevolg dat het voor bestuurders en developers op dit moment onvoldoende duidelijk is wat nu precies van hen wordt verwacht. Om cyberrisico's het hoofd te kunnen bieden is het van belang dat deze nadere invulling op korte termijn komt.

197 https://www.ncsc.nl/documenten/publicaties/2021/juni/28/handreiking-cybersecuritymaatregelen

Attentiepunten

- Security by Design is een belangrijk instrument bij het weerbaar maken van een organisatie tegen cybercriminaliteit; hoe eerder security vraagstukken worden meegenomen in het ontwikkeltraject, des te meer impact de maatregelen zullen hebben;

- De AVG gaat uit van accountability. Het is dan ook van belang te documenteren op welke wijze aan de verplichting van Privacy & Security by Design is voldaan;

- Bij een gebrek aan concrete handvatten voor de concrete invulling van Privacy & Security by Design doen organisaties en bedrijven er vooralsnog goed aan de bestaande richtlijnen/baselines te volgen, aangevuld met een risicoanalyse op organisatieniveau;

- Bestuurders van verwerkingsverantwoordelijken zijn verantwoordelijk voor een adequate omgang met digitale risico's;

- Zolang de verplichting van Privacy & Security by Design zich niet (ook) rechtstreeks tot developers en aanbieders van software richt, is het zaak concrete eisen te stellen aan developers en aanbieders (en deze eisen weer te documenteren in het kader van accountability).