

Om technische producten cyberveilig te maken, is een cultuurverandering nodig

Security by design is een belofte in cybersecurity. Rick van der Kleij (TNO/ Avans hogeschool) betoogt in deze blogbijdrage dat voor het inlossen van deze belofte om veiligheid door ontwerp na te streven een cultuurverandering nodig is. Maar hoe zet je die cultuurverandering in gang?

[Cybersecurity](#)[Weerbaarheid](#)[Cultuur](#)



De Europese Commissie heeft nieuwe cyberbeveiligingsregels voorgesteld voor veiligere producten via de [Cyber Resilience Act](#) (CRA). De voorgestelde CRA legt cyberbeveiligingsverplichtingen op aan alle producten met digitale elementen. Bovendien introduceert de CRA een wettelijke verplichting tot [security by design](#) (SbD).

Het idee achter SbD is dat veel beveiligingsproblemen kunnen worden voorkomen door producten met digitale elementen zo te bouwen dat ze bescherming bieden tegen kwaadwillige cyberactoren voordat ze worden ingezet in een operationele omgeving in de echte wereld. Misschien herinnert u zich nog de hack van beveiligingscamera's en videobabyfoons jaren geleden waardoor live beelden van

deze camera's massaal gedeeld werden [op internet](#). Veelal doordat kwetsbaarheden in de software konden worden uitgebuit om ongeoorloofde toegang te verkrijgen. En ook levenskritieke systemen zoals pacemakers en insulinepompen zijn volgens experts kwetsbaar voor hacks door [gebrekkige ingebouwde beveiliging](#). Softwareontwikkelaars houden daarom idealiter vanaf het begin rekening met beveiliging.

Een beveiligingsmentaliteit bij ontwikkelaars is een goede stap voorwaarts. Maar het is zeker geen wondermiddel voor meer cybersecurity, tenzij het ontwikkelteam integraal verantwoordelijk wordt gesteld voor de digitale veiligheid in al haar facetten. Want een (te) eenzijdige aandacht voor technische aspecten van security kan ook leiden tot onbruikbare security. Onbruikbare security zorgt uiteindelijk altijd voor olifantenpadjes in het gebruik, met onveilige situaties tot gevolg. Zo kan het zijn dat een beveiligingscamera veel veiligheidsinstellingen heeft, maar deze niet worden gebruikt omdat ze het gebruiksgemak in de weg staan, waardoor de gebruiker nog steeds het risico loopt om slachtoffer te worden van een hack. Zie hiervoor ook [mijn vorige blog](#), over de rol van de mens in het veiligheidssysteem.

Stimuleren integrale kijk op veiligheid

SbD is dus meer dan alleen veiligheid door ontwerp. SbD zou ook aandacht voor gebruiksvriendelijkheid moeten omvatten. Maar hoe doen we dat? Hoe zetten we een transitie in beweging naar een meer integrale kijk op veiligheid binnen ontwikkelteams met een overwegend technische oriëntatie? Want er is nog steeds weinig aandacht voor het veilig en gebruiksvriendelijk ontwikkelen van producten met digitale elementen. In veel conventionele projecten worden veiligheid en gebruiksvriendelijkheid niet beschouwd als primaire doelen en (dus) vaak geofferd in het proces om deadlines te halen tegen minimale kosten.

Maar er gloort hoop aan de horizon. Onderzoeken [laten zien](#) dat er een relatie is tussen de bedrijfscultuur en het nastreven van veiligheid en gebruiksvriendelijkheid door ontwerp. Bedrijfscultuur wordt gereflecteerd door het gedrag van medewerkers. Dit gedrag wordt beïnvloed door het implementeren van specifieke componenten door de organisatie, zoals kledingvoorschriften, processen of technische maatregelen. Om de hier besproken gewenste integrale kijk op veiligheid te cultiveren in ontwikkelteams, kunnen organisaties ervoor zorgen dat een relevante en adequate set van componenten wordt geïmplementeerd. In de literatuur worden verschillende van deze [componenten genoemd](#). Ik bespreek er hier drie, namelijk leiderschap, beleid en bewustzijn.

Cruciale rol leiderschap

Leiderschap speelt een cruciale rol (hieronder valt ook goed ondernemerschap). Zonder commitment en investeringen vanuit de top van het bedrijf is een transitie naar een integrale beveiligingsmentaliteit in het ontwikkelproces kansloos. Leidinggevendens kunnen de cultuur beïnvloeden door een duidelijke visie en waarden te communiceren die de gewenste cultuur weerspiegelen. Door consistent te zijn in het benadrukken van deze elementen in communicatie en besluitvorming, kunnen leidinggevendens de leden van ontwikkelteams inspireren om de

verantwoording te nemen voor de ontwikkeling van een veilig en gebruiksvriendelijk product in al haar facetten.

Ook via beleid kunnen organisaties een krachtige invloed uitoefenen op de cultuur. Bijvoorbeeld door het vaststellen van ontwikkelrichtlijnen die gewenst handelen bevorderen en ongewenst gedrag ontmoedigen in ontwikkelteams. Dit kan variëren van ethische richtlijnen, regels met betrekking tot het schrijven van veilige code, het betrekken van eindgebruikers vroeg in het ontwikkelproces tot een beloningssysteem dat in lijn is met de gewenste cultuur.

Door ontwikkelaars meer bewust te maken van het belang van gebruiksvriendelijkheid en informatiebeveiliging in productontwikkeling en hen te voorzien van relevante training kan de gewenste cultuur worden bevorderd. Zorg ervoor dat de training regelmatig wordt geüpdatet en dat ontwikkelteams op de hoogte blijven van de verschillende perspectieven op SbD. Of zorg ervoor dat je ontwikkelaars benoemt of aanstelt in de teams met kennis van gewenste perspectieven op bijvoorbeeld veiligheid. De zogenaamde 'security champions': ontwikkelaars die snappen wat erbij komt kijken, security-bewust zijn en onderdeel uitmaken van het [development team](#).

Tot slot

Door cultuurcomponenten zoals leiderschap, beleid en bewustwording strategisch in te zetten en op een constructieve manier te gebruiken, kunnen bedrijven de transitie naar een integrale benadering van veiligheid in hun ontwikkelteams positief beïnvloeden. Dit draagt bij aan de ontwikkeling van producten die digitaal veiliger zijn zonder dat daarbij de gebruikservaring wordt belemmerd met meer cyberweerbaarheid als resultaat.

Mijn streven is een consortium te bouwen waarin we inzichten ontwikkelen en toepassen die organisaties en ontwikkelteams kunnen helpen in deze transitie bij het ontwikkelen van veiligere producten. Meer weten of goede ideeën? Neem contact op via Rick.vanderkleij@tno.nl of R.vanderkleij1@Avans.nl.

Rick van der Kleij is lector Cyberweerbare Organisaties bij Avans hogeschool en sr. cybersecurity onderzoeker bij TNO.

[Dutch IT Leaders - Om technische producten cyberveilig te maken, is een cultuurverandering nodig](#)