Auteur: Dr. Els de Busser is universitair docent cyber security governance bij het Institute of Security and Global Affairs van Universiteit Leiden. Els is bereikbaar via: e.de.busser@fgga.leidenuniv.nl.

Cybersecurity by integrated design: veiligheid voorbij technologie

Storingen in het functioneren van digitale technologie en de gevolgen van hacks of datalekken worden vaak pas aangepakt wanneer er effectief schade is veroorzaakt. We denken in dergelijke gevallen dan voornamelijk aan financiële of materiële schade. Het is van groot belang de aanpak van zulke problemen te verschuiven naar de vroegste ontwikkelingsfase. De toeslagenaffaire liet op pijnlijke wijze zien hoe fouten in de ontwikkeling van digitale technologie tot meer dan enkel financiële of materiële schade kunnen leiden (1).

Het door NWO gefinancierde onderzoeksproject Cybersecurity by Integrated Design – kortweg het C-SIDE project – heeft als ambitie richtlijnen op te stellen voor softwareontwikkeling. Deze richtlijnen houden rekening met zowel technologische als niet-technologische aspecten. Het doel is om al in de beginfasen van softwareontwikkeling meer veiligheid in te bouwen, zodat dit later resulteert in veiligere technologie.

Een interdisciplinair team van wetenschappers van de Universiteit Leiden en de Haagse Hogeschool bestudeert verschillende elementen van dit proces. Hun doel is om een set richtlijnen te creëren die sleutelfiguren in het softwareontwikkelingsproces helpt. Deze richtlijnen zullen hen ondersteunen bij het integreren van relevante organisatie-gerelateerde aspecten, mensenrechten en het voorkomen en detecteren van kwetsbaarheden in softwaredesign. Bovendien omvat het project een studie naar het meten van veiligheid en kwetsbaarheden in technologie. Om het gebruik van zulke richtlijnen te ondersteunen, wordt ook een studie uitgevoerd naar het institutionele design van de Nederlandse overheid.

Waarom digitale veiligheid door geïntegreerd design?

By-design denken is op zichzelf niet nieuw. Privacy-by-design en security-by-design zijn veelvoorkomende begrippen in de wereld van digitale technologie en veiligheid. Wat wel nieuw is, is om het by-design denken uit te breiden naar meer dan enkel de technologische aspecten. De holistische en interdisciplinaire aanpak van het C-SIDE project past daar uitstekend bij. Door expertises uit verschillende disciplines bij elkaar te brengen zoals de computerwetenschappen, sociale wetenschappen, politieke wetenschappen en organisatiestudies, krijgen we een breder beeld van wat nu precies nodig is om software niet alleen op technologisch vlak beter en veiliger te ontwikkelen, maar ook hoe de organisatie rondom de softwareontwikkelaar optimaler en veiliger kan werken. We hebben het dan zowel over de organisatie van het ontwikkelende bedrijf, als over hoe de overheid zich organiseert. Vanuit wetenschappelijk standpunt is het project innovatief, omdat het onderzoekers van diverse disciplines samenbrengt om gezamenlijk iets nieuws te creëren. Een grote uitdaging voor de projectleiding is om vier promovendi hun eigen onderzoek te laten doen. Tegelijkertijd moeten zij in teamverband de richtlijnen ontwikkelen, zodat het geheel meer waarde heeft dan de som der delen.

Veiligheid voorbij technologie

Security-by-design mag dan wel een veelgebruikt begrip zijn in de ontwikkeling van technologie, uit een systematisch onderzoek naar de wetenschappelijke literatuur over security-by-design blijkt echter dat er vooral onduidelijkheid heerst over wat dit nu precies betekent (2). Een discipline-overstijgend onderzoek geeft aan dat er geen eensgezindheid bestaat over het begrip. In tegenstelling tot privacy-by-design dat door slechts één auteur uitvoerig werd bestudeerd en beschreven, is security-by-design door een groot aantal auteurs geanalyseerd, met een brede variatie aan definities tot gevolg. Auteurs zijn het oneens over wat nu precies beschermd wordt – toestellen, systemen, of privacy – en wat nu precies vermeden wordt door security-by-design toe te passen – kwetsbaarheden, aanvallen of dreigingen. Ook de manier waarop, en op welk moment in de software lifecycle security-by-design wordt ingezet, is niet geharmoniseerd. Wat wel duidelijk is, is dat er een onmiskenbare gelegenheid bestaat om security-by-design concreteer te maken door een eenduidige definitie en bruikbare richtlijnen aan te bieden. Dit is wat het C-SIDE project beoogt.

Digitale veiligheid wordt vaak beperkt ingevuld op basis van de traditionele triade: vertrouwelijkheid, integriteit en beschikbaarheid, ook wel bekend als de 'CIA'. Wanneer deze klassieke blik echter verder wordt geopend, en ook fysieke en sociale veiligheid worden meegenomen in het denken over security-by-design, kan dit resulteren in een verhoogde aandacht voor de impact die technologie op mensen kan hebben, bijvoorbeeld door algoritmes te ontwerpen die niet discriminerend werken. Een andere manier om security-by-design breder in te vullen is door te kijken naar de waarden die een softwareontwikkelingsbedrijf vooropstelt, zoals privacy, inclusie, en duurzaamheid. Deze waarden vloeien namelijk door in de geldende regels, processen, en uiteindelijk de producten die het bedrijf op de markt brengt. Een bedrijfscultuur is ook gebaseerd op deze waarden en heeft volgens wetenschappelijk onderzoek (3) een effect op de veiligheid in het bedrijf. Dit betekent dat wanneer werknemers van een bedrijf zich veiliger gaan gedragen en veiligheid een rode draad vormt door de besluitvormingsprocessen heen, en de praktijk in alle lagen, dat betere resultaten oplevert dan wanneer enkel wordt gefocust op het naleven van de geldende wet- en regelgeving. Wanneer bijvoorbeeld de sociale veiligheid sterk is in een organisatie, en werknemers voldoende vertrouwen hebben om op ondeugdelijkheden in softwareontwikkeling te wijzen zonder negatieve gevolgen, dan leidt dit tot veiligere technologie.

Een (overdreven) focus op het naleven van geldende wet- en regelgeving kennen we als compliance. Vaak wordt echter de denkfout gemaakt dat compliance automatisch tot veiligheid leidt (4). Mensen zullen fouten blijven maken, ongevallen zullen

Digitale veiligheid wordt vaak beperkt ingevuld op basis van de traditionele triade: vertrouwelijkheid, integriteit en beschikbaarheid, ook wel bekend als de 'CIA'

blijven gebeuren en ook een hacker zal er niet bij stilstaan of een bedrijf een perfecte compliance-score heeft.

Het C-SIDE project bouwt verder op deze visie en breidt ook hier het concept van veiligheid uit. Het uitbreiden van veiligheid met fysieke en sociale veiligheid werd tot op zekere hoogte bevestigd door een steekproef van softwareontwikkelaars (5). Op de vraag wat we precies van hen mogen verwachten als het gaat om het inschatten van de impact van de software die zij ontwikkelen, kan daar onmogelijk een algemeen antwoord op gegeven worden. Dit kan enkel op basis van concrete omstandigheden. Een mogelijk criterium dat hierbij kan helpen is de 'redelijkerwijs te verwachten impact', rekening houdend met de technologische en maatschappelijke ontwikkelingen van dat moment, om een juiste inschatting te kunnen maken.

Een belangrijke technologische tak van het C-SIDE project is het meten van veiligheid. Naast het veelgebruikte meten van het aantal kwetsbaarheden, is het vernieuwende van het project dat ook de kritische inzichten van de betrokken personen worden meegenomen in het meten van veiligheid (6). Dit zorgt voor een meer geïntegreerde aanpak. In het meten van veiligheid, door middel van het nagaan van het aantal kwetsbaarheden in software, wordt vaak vertrouwd op zogenaamde bibliotheken van bekende kwetsbaarheden. Een tweede technologische tak van het C-SIDE project betreft daarom een analyse van de kwaliteit en kwantiteit van dergelijke bibliotheken, en wat de mogelijkheden voor het verbeteren van deze bibliotheken zijn om uiteindelijk tot veiligere software te komen.

De combinatie van technologie en governance in het project doet ook de vraag rijzen hoe de Nederlandse overheid een passende ondersteuning kan bieden van een geïntegreerde aanpak van digitale veiligheid. Om deze vraag te beantwoorden werd in een eerste fase van het project het Nederlandse overheidslandschap van digitale veiligheid in kaart gebracht. In een tweede – nog lopende fase – wordt bestudeerd in hoeverre dit landschap gefragmenteerd is, en of dit problematisch is. Een belangrijk onderdeel van deze studie is hoe de academische literatuur en de beschikbare beleidsdocumenten schrijven over fragmentatie.

De C-SIDE richtlijnen

Nu het onderzoeksproject inmiddels halverwege is, neemt het eindproduct duidelijkere vormen aan. De richtlijnen die na vier jaar wetenschappelijk onderzoek worden gepubliceerd, zijn onderverdeeld op basis van de verschillende belanghebbenden over digitale veiligheid: de Nederlandse overheid, softwareontwikkelaars, en de bedrijven waarvan ze deel uitmaken. Door deze belanghebbenden heldere richtlijnen aan te reiken die een organisatorische, technologische, ethische, en beleidsmatige inbedding van veiligheid mogelijk maken, is het doel van het C-SIDE project, een geïntegreerde en interdisciplinaire aanpak van digitale veiligheid na te streven, een stap dichterbij.

Referenties

(1) Prins, C. (2021), Discriminerende algoritmes, Nederlands Juristenblad: https://www.njb.nl/blogs/discriminerende-algoritmes/

(2) Del Real, C.; De Busser, E. en Van den Berg, B. (2024). Shielding Software Systems: A Comparison of Security by Design and Privacy by Design Based on a Systematic Literature Review, Computer Law and Security Review, Vol. 52, 105933.

(3) Schein, E.H. (1990). Organizational culture. Am. Psychol., Organizational Psychology 45, 109–119; Van Niekerk, J.F. en Von Solms, R. (2010). Information security culture: A management perspective. Computer Law and Security Review, Vol. 29, 476–486.

(4) Boeken, J. (2024). From Compliance to Security, Responsibility beyond Law, Computer Law and Security Review, Vol. 52, 105926.

(5) Del-Real, C., en De Busser. (2023). Defining security by design: A stakeholders perspective. Cyber Security by Integrated Design. December 2023: https://www.projectcside.nl/research-and-publications

(6) Kudriavtseva, A. (2024). A Software Security Evaluation Framework. In2024 IEEE/ACM 46th International Conference on Software Engineering: Companion Proceedings (ICSE-Companion '24), April 14–20, 2024, Lisbon, Portugal. ACM, New York, NY, USA (in druk)