Boekbespreking

Agile secure software lifecycle management, secure by agile design

22 september 2020

Jean-Jacques Bistervels

Het is natuurlijk al een tijdje een 'hot topic': agile ontwikkelen. Het boek beschrijft op een compacte wijze de basisconcepten die ten grondslag moeten liggen aan een *veilige* agile-ontwikkelaanpak. Het is opgesteld onder regie van de Secure Software Alliance (SSA) en uitgegeven onder de vlag van ISACA. Het is gratis te downloaden.[1]

Auteurs Barry Derksen, Monique Neggers, Danny Onwezen, Stef Zelen

Titel Agile secure software lifecycle management, secure by agile design

Uitgever en jaar van uitgave Business & IT Trends Institute, 2019

ISBN 9789081786652

De inhoud – Sprints

Het boek is – hoe kan het ook anders – opgedeeld in 'sprints'. In totaal acht, om precies te zijn.

Na een korte inleiding, waarin de schrijvers aangeven waarom de bestaande frameworks als ISAE 3402 of ISO27001 onvoldoende houvast geven voor het ontwikkelen van *veilige* software, starten de schrijvers met Sprint 1: de basis van het raamwerk dat SSA heeft ontwikkeld om meer houvast te geven.

In Sprint 2 benadrukken de schrijvers dat ontwikkelaars moeten kunnen denken als een hacker. Dat betekent voor veel teams een zekere cultuuromslag. Ze maken duidelijk dat het expliciteren van *security requirements* nodig blijft, ook binnen een *agile mindset*. De weg om er te komen, krijgt binnen de agile-aanpak een wat andere invulling.

Sprint 3 beschrijft vervolgens een aantal belangrijke ontwikkelingen in de periode 2016-2020 die *full swing* onze IT-omgevingen hebben veranderd. Samengevat wordt dit de 'SMAACT' genoemd: Social, Mobile, Analytics, Agile, Cloud en Internet of Things. Niet dat zij voor die tijd onbekenden waren, maar ze zijn pas de laatste jaren echt doorgebroken binnen de (IT-)organisaties die agile zijn gaan werken. Ze dienen hier als context die verschijnselen helpt te begrijpen, zoals de doorbraak van agile binnen het ontwikkeldomein, de druk op 'security' en het waarom van het belang van veilige software en systemen.

Sprint 4 en 5 beschrijven de fundamenten voor veilige softwareontwikkeling. Een must-read voor de IT-auditors die zich hier verder in willen verdiepen om niet te hoeven terugvallen op de 'oude' theorie, die niet bruikbaar is in agile-omgevingen.

Sprint 6 en 7 ten slotte, behandelt het Agile Secure Software Development Lifecycle-model.

Sprint 8 voegt als bonus ook nog een roadmap toe voor veilige software in hardware (*embedded*) en bij toepassing voor Internet of Things.

Allesomvattend?

Missen we dan nog wat? Een compact boek betekent vanzelfsprekend dat niet alles aan bod komt. Deze publicatie geeft dan ook een overzicht in vogelvlucht. Maar als ik dan toch iets moest toevoegen, dan zou ik een uitbreiding opnemen die ingaat op hoe deze aanpak toe te passen binnen de omgeving voor de interne *Enterprise systems*, ofwel de standaard IT-pakketten waaraan natuurlijk ook veel gesleuteld wordt. Deze omgeving zal op onderdelen toch een wat bijgestelde variant behoeven door de specifieke kenmerken van standaard IT-pakketten. Bijvoorbeeld omdat de nadruk bij verificatie meer of checks van de juiste configuratie ligt, er geheel andere 'bedreigingen' spelen, of dat in dergelijke teams de verantwoordelijkheid over de gehele IT-stack vaak is verdeeld over verschillende afdelingen. Wat weer een andere rolinvulling in de governance nodig kan maken.

Conclusie: verplichte kost

Kortom: een lezenswaardig boek dat op beknopte wijze inzicht geeft in de noodzakelijke basisvereisten om betrouwbare en veilige software te kunnen ontwikkelen in de agile context. Leest prettig en snel, en heeft een logische en duidelijke opbouw. Kortom, 'Agile secure software lifecycle management; Secure by agile design' zou een basiswerkje moeten zijn, verplichte kost voor alle IT-auditors.

NOOT

[1] https://securesoftwarealliance.org/agile-secure-software-lifecycle-management-secure/, geraadpleegd' op 26-07-2020, ECP

Ir. J.E. (Jean-Jacques) Bistervels RE CIA CCSA CRISC CDPSE CCP | informatiebeveiligingsmanager en privacyspecialist bij *Sanoma*

Jean-Jacques Bistervels is werkzaam als Informatiebeveiligingsmanager bij Sanoma. Daarnaast houdt hij zich bij Sanoma bezig met fraudebeheersings- en privacyvraagstukken. Na zijn studie Technische Bedrijfskunde aan de TUE is hij zijn carrière bij Ernst & Young gestart als IT-auditor. Hij heeft daarna ruim zeven jaar gewerkt binnen de farmaceutische sector en daarna ruim tien jaar in de financiële sector. Binnen NOREA is hij actief voor de kennisgroep Software Development en als redacteur voor de IT-auditor.