

On the Design and Engineering of a Zero Trust Security Artefact

Yuri Bobbert¹ & Jeroen Scheerder²

¹University of Antwerp and ON2IT, Netherlands

²ON2IT, Netherlands

yuri.bobbert@on2it.net, jeroen.scheerder@on2it.net

Abstract. Adequately informing the board of directors about operational security effectiveness is cumbersome. The concept of Zero Trust (ZT) approaches information and cybersecurity from the perspective of the asset, or sets of assets, to be protected, and from the value that it represents. Zero Trust has been around for quite some time. This paper continues on the authors previous research work on the examination of Zero Trust approaches, what is lacking in terms of operationalisation and which elements need to be addressed in future implementations and why and how this requires empirical validation. In the first part of the paper, we summarise the limitations in the state of the art approaches and how these are addressed in the Zero Trust Framework developed by ON2IT ‘Zero Trust Innovators’. Then we describe the design and engineering of a Zero Trust artefact (dashboard) that addresses the problems at hand, according to Design Science Research (DSR). The last part of this paper outlines the setup of an empirical validation trough practitioner-oriented research, in order to gain a better implementation of Zero Trust strategies. And how this validation was conducted in 2020 with 73 security practitioners. The final result is a proposed framework and associated technology which, via Zero Trust principles, addresses multiple layers of the organization to grasp and align cybersecurity risks and understand the readiness and fitness of the organization and its measures to counter cybersecurity risks.

Keywords: Zero Trust Security, Architecture, Cybersecurity, Digital Security, Managed Security Services (MSS), Security Operation Centre (SOC), Security Strategy, Design Science Research (DSR), Group Support System (GSS), Platform technology, Security Orchestration, Automation and Response (SOAR).

1 Introduction

These days it’s impossible to imagine business without technology. Most industries are becoming “smarter” and more tech-driven — ranging from small individual tech initiatives to complete business models with intertwined supply chains and "Platform" based business