CLOUDSCAPE BRAZIL POSITION PAPER

Title: CloudWATCH2 – Helping cloud service customers become security-savvy through risk management profiling

Authors: Jesus Luna, Cloud Security Alliance, Nicholas Ferguson, Stephanie Parker and Gennaro Fontanarosa, Trust-IT Services

Focus area:

Cloud computing has now reached a point where it is truly accessible to all types of organisations. However, many small and mid-sized organisations often lack IT expertise to assess security measures of cloud service providers and monitor the levels actually delivered. CloudWATCH2 fills this gap with a risk management profile that guides cloud service customers through security self-assessments.

Who stands to benefit and how:

Cloud computing has become pretty much a staple in the start-up and SME culture because it radically reduces barriers to entry in almost any sector without the need for upfront investments. Many of these small firms, however lack the expertise to assess and monitor the security measures of a cloud service provider necessary to protect their data and business assets in an increasingly digital economy.

Herein lies the value of CloudWATCH2, a coordination and support action funded under Horizon 2020 for software, services and cloud computing (DG CONNECT Unit E2). In order to increase awareness of cloud security and help small firms and IT teams in government agencies monitor security levels, CloudWATCH2 provides a simple, efficient and inexpensive approach to identifying and managing their cloud security risks from both a technical and organisational perspective. The approach is standards-based, leveraging standards developed by the US National Institute of Standards and Technology (NIST) and the International Standardization Organization/International Electrotechnical Commission (ISO/IEC).

Position paper:

Compliance with business, regulatory, operational and security requirements largely depends on the service and deployment model and the cloud architectural context. It is therefore imperative that all levels of an organisation understand their responsibilities for adequate cloud security and for managing information system-related security risks. The result is a risk profile that guides cloud service customers through security self-assessments.

The approach taken by CloudWATCH2 takes into account security requirements elicited through relevant studies in Europe and globally and is instantiated on top of a well known best practices of the Cloud Security Alliance, namely the Cloud Control Matrix (CCM) and the enterprise Architecture (EA). Both are widely used industrial practices and have been mapped to relevant standards like NIST 800-53v4 and ISO/IEC 27002.

There are many benefits for small firms and IT teams in public administrations (PAs) and government agencies.

Simplicity: the guided self-assessment for SMEs and Public Administrations means they do not need expert knowledge of cloud security.

Technical and organisational focus: SMEs and Public Administrations are guided in the elicitation of security controls considered “good enough” for their requirements. These controls are based on the Cloud Security Alliance Cloud Control Matrix (CCM) and cover both technical and organisational aspects of the cloud customer.

Repeatable process: SMEs and Public Administrations can periodically re-assess their risks to identify opportunities for improving their risk profile.

Standards-based: CloudWATCH2 leverages well-known standards and best practices to facilitate industrial uptake, with the Cloud Control Matrix and Enterprise Architecture both based on international standards from ISO/IEC and NIST.

High automation potential: facilitating the development of software applications to empower SMEs and Public Administrations in creating and using risk profiles.

Cloud specific: to the best of our knowledge, there are no other approaches aimed at developing cloud-specific risk profiles.

CloudWATCH2 Risk profiles for the public sector and SMEs

The CloudWATCH2 project has just published its first report on risk-based decision making mechanisms for cloud service in the public sector. The report outlines the challenges and requirements for this sector and a methodological approach for creating and using risk profiles. This includes three well-identified steps covering the whole security lifecycle from a risk-management perspective. Final results and a risk profile for SMEs will be published in 2017.

Links

www.cloudwatchhub.eu, @CloudWatchHub

Report: Risk-based decision making mechanisms for cloud service in the public sector – http://www.cloudwatchhub.eu/risk-profile-for-public-sector-report

https://cloudsecurityalliance.org/group/cloud-controls-matrix/